E-voting Platform based on Ethereum Decentralised Network

Thesis submitted in partial fulfillment of the requirements
for the degree of

Dual Degree Engineering
By

Rishi Srivastava
Registration No- 1471077016

Supervised by
Dr. Rourab Paul

Department of Computer Science and Engineering

Department of Computer Science and Engineering
Institute of Technical Education and Research, BBSR
Siksha 'O' Anusandhan(Deemed To Be University)
Bhubaneswar, Odisha, India

2019

INSTITUTE OF TECHNICAL EDUCATION & RESEARCH, BHUBANESWAR

DISSERTATION APPROVAL CERTIFICATE

This is to certify that the Thesis entitled "***E*-voting Platform based on Ethereum Decentralised Network**" is a bonafide work done by **Rishi Srivastava** bearing Regd.No.**1471077016** of 10th semester, **Department of Computer Science Engineering**, towards the completion and award of DDE(B.Tech and M.tech) from **ITER**, under **Siksha 'O' Anusandhan Deemed to be University, Odisha**.

HOD :	**Project Coordinator:**	**Guide:**
Dr.Debahuti Mishra Professor & HOD Dept. of CSE	Dr.Kaberi Das Assistant Professor Dept. of CSE	Dr.Rourab Paul Assistant Professor Dept. of CSE

External Examiner:

Signature

DECLARATION

I declare that every parts of this Project Report is genuinely my work and has not been submitted for any other degree. I acknowledge that if any sort of malpractice is detected in relation to this report I shall be held liable for it.

Submitted by
Rishi Srivastava
Regd No. 1471077016
M.Tech(CSE)
Dept. of CSE

ACKNOWLEDGEMENT

I avail this opportunity to express my profound sense of gratitude to Asst.Prof. Mr. Rourab Paul for his constant supervision, guidance and encouragement right from the beginning till the completion of the seminar.

I wish to thank all the members of faculty of CSE department for their valuable advice and encouragement. Last but not the least a special thanks to all my colleagues for their support and compassion.

Rishi Srivastava
Regd No. 1471077016
DDE M.Tech(CSE)

Abstract

Conventional voting system is very complex and time taking process that consumes a very large amount of fund and manpower which reduces its efficiency. Decentralized Application based on Ethereum blockchain network enables us to provide safe and secure way to organise a digitally verified platform to conduct an efficient voting system. In our submission we provide a basic architecture of Ethereum blockchain network that provide a smart way to conduct e-voting that overcome most of the issues of conventional system with higher efficiency and security.

Contents

1 Introduction **1**

1.1 Blockchain 1

1.1.1 Traditional voting system in India 2

1.2 How Does The Application Work 3

1.2.1 Centralised Network 3

1.2.2 Decentralised Network 5

1.2.3 Hash algorithm 5

2 *A*ppliation **7**

2.1 Blockchain based Applications That Are Transforming The World 8

2.2 Issues in Blockchain Network 8

2.3 Motivation 10

2.4 Objectives of Our Research 11

2.4.1 The objective of our research also includes: . . 11

2.5 Organization of The Thesis 13

3 Literature Review **14**

4 Methodology of the application **16**

4.1 Ethereum 16

4.2 Differences Between Ethereum and Bitcoin 16

4.3 The characteristics of a decentralized Ethereum Blockchain Network 17

4.4 Downside of decentralized Ethereum applications . . 17

4.5 Smart contracts 18
4.6 Implementation of work 18
4.7 Installing Dependencies 18
4.7.1 Ganache 18
4.7.2 Truffle Framework 19
4.7.3 Metamask Ethereum Wallet 20

5 Implementation **22**
5.1 Ganache Personal Blockchain 22
5.2 Writing our smart contract 24
5.3 Result Of The Implementation and Testing 24

6 Conclusion **28**

List of Figures

1.1 Work flow diagram 3
1.2 web application network 4
1.3 DAP Network 6

2.1 Applications 7

4.1 E-Voting Homepage 19
4.2 Flow Diagram 21

5.1 Ganache Homepage 22
5.2 election homepage 24
5.3 client side -index.html 25
5.4 Now your front-end application should look like this: 25
5.5 result 26

Chapter 1

Introduction

People often think of Blockchain as a transaction system for virtual currency i.e cryptocurrency, but if we look closer and research about it then the actual potential of this, It has extreme potential that we should never underestimate.We'll see that it's a ground-breaking technology for which monetary transaction use is just one of the possible applications. As the name, The blockchain is a chain of blocks that each block contain different information.

1.1 Blockchain

Technically, It is a distributed database system that provide a continuously increasing list of transactions called blocks. Every block has a information such as a block header, the digital identity including the hash of the block and hash of the previous block, a timestamp, and other transaction information.

Blockchain is a concept where distributed and decentralised computers systems or nodes that is used to record all trasanction across system so that the data can not be altered without altering all the nodes.They communicate to one another through chain of distributed system. Each network participant have a copy of the code and the data on the blockchain. All of this data is contained records called blocks which are basically chained together to make up the

blockchain. All of the nodes on the blockchain network ensure that this data is safe, secure and unbreachable, unlike a centralized database application where the code and data can be breached or change at any point of time time. Thats makes the blockchain so dependable and powerful. Another important difference between centralised and decentralised applications is that instead of being a user of the any application, you are a user of the blockchain network itself.

1.1.1 Traditional voting system in India

Conventional voting platform in the India and around the world, has been a matter of threat for several reasons.

- The complex process as well as the human errors is very common while counting the votes.
- People generally avoid going to booths because of many constraints, also turnout rate are even lower in state and local elections.
- Voter authentication is a major issue in India from several decades.Nevertheless Electronic voting machines (EVM) have been adopted in the India over 90s. However EVM are always a controversial topic over all the election as the vote counts are not auditable by the public. Hence it failed to gain the confidence of the general public.

Now the decentralised application based on blockchain network, if it is regulated for the voting purposes, it could completely change the structure of the voting process because the technology itself is open in terms of how it works and because of open-source implementation. It will enable voters to verify his/her votes and allow to verify the votes, also counting wold be completely automatic without any human interference which result in reduce of any dispute or any claim of rigged election.

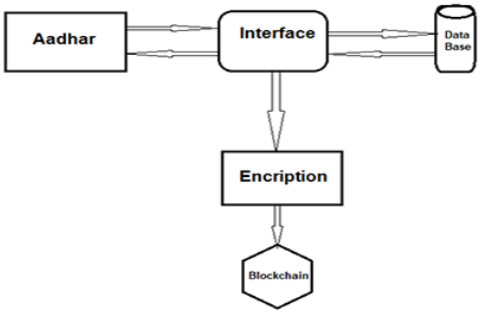

Figure 1.1: Work flow diagram

1.2 How Does The Application Work

1.2.1 Centralised Network

Generally we interact with a web sites over internet, we use a web browser to connect to a centralised databse server through a network. The server consists all the back-end code as well as all the data into its database. Anytime we connect with application, We must have to communicate with this central server through a network.

Lets look at a web application.

Problem we face in the centralise structure:

- Database could be changed or tempered.
- The source code that inside the web server could also be changed at any time as it is in control of a centralised system.

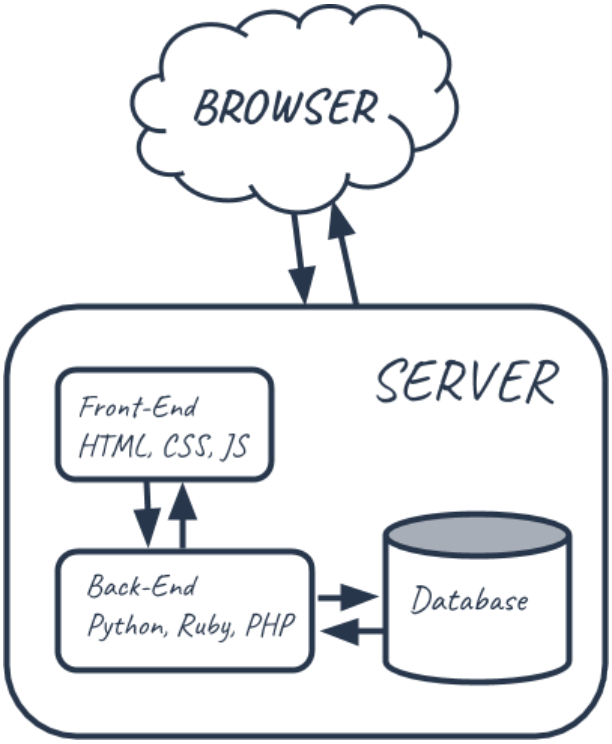

Figure 1.2: web application network

1.2.2 Decentralised Network

Instead of having a centralised database network system, the blockchain is a distributed decentralised network. It is a peer-to-peer network of computers system, called nodes, each node or peer communicate to other node. The purpose of node is to validate unverified recent mined blocks. So, There would be no any central servers. Just a group of computer nodes that communicate to one another over the same network.Every block or node has its own unique identity i.e called a hash, that can identify all the content of the block.

1.2.3 Hash algorithm

Hash algorithm is mathematical encryption function that generate a hash value from a base input using some complex hashing algorithm. It is impossible to predict or extract the original input value without knowing the information used to create a hash value. for example if we take a input like "1234", and a hash function "zxy123rm" its hash value suppose "10056". So here we can observe it is impossible to crack the real input i.e "1234" from its generated hash value "10056" .

Hashing algorithm is the backbone of the decentralised application world as it contains uncrackable encryption technology.

The structure of the decentralised application.

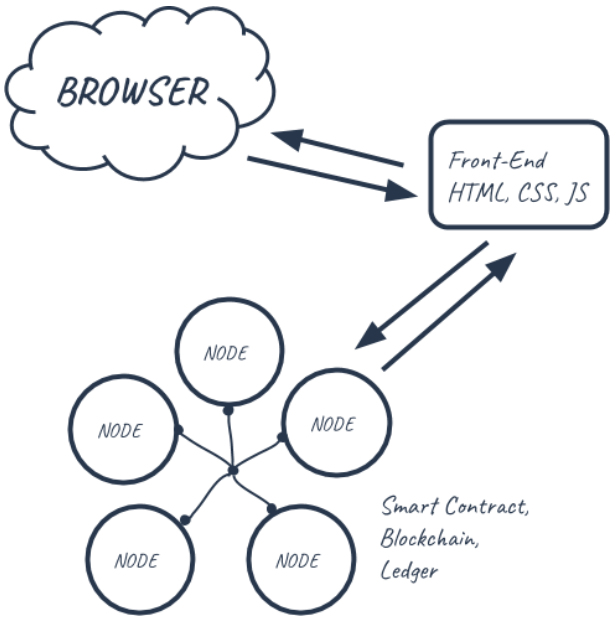

Figure 1.3: DAP Network

Chapter 2

*A*ppliation

Blockchain is a term that acknowledge different things to different people:-

- For the developer,It consists of a set of protocols and encryption technology for storing data on a distributed network securely.
- For finance and businesses, it is a distributed ledger and technology of new digital "crypto currencies".
- For technologists, it is a driving force behind the next generation of the internet.
- For others, it is tool for reshaping society and economy that taking us into more decentralized world.

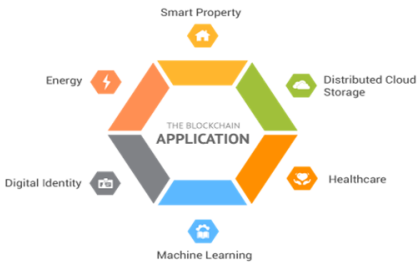

Figure 2.1: Applications

2.1 Blockchain based Applications That Are Transforming The World

- Asset Management: Trade Processing and Settlement
- Personal Identification
- Insurance: Claims processing
- Transaction: Cross-Border Payments
- Internet-of-Things (IoT)
- Smart Household Appliances
- Blockchain Identification
- Birth, wedding, and death certificates
- Passports

2.2 Issues in Blockchain Network

Every technology has its positive as well as some downside which we try overcome using different techniques, It has ability to create a secured world of digital identity that can transform many industries over the next period but some the issue still needs to eliminate by doing deep research work, here we are indicating about the fields which we find during our research work:-

- **Regulation**:- Regulations have always struggled to keep up with advances in technology. Since this technology directly bypass the central authority or regulation completely. There is thus a strong argument for blockchain applications to work within existing regulatory structures

- **Security and privacy**:- Many potential applications of the blockchain require smart transactions and contracts to be indisputably linked to known identities, and thus raise important questions about privacy and the security of the data stored and accessible on the shared ledger.
- **The Criminal Connection**:- The anonymous feature of the blockchain technology attracted not only experts but also criminal personals. Why? Well, the nature of the network is decentralized so that no one can know your true identity.
- **Energy Consumption:-**Energy consumption is another blockchain adoption challenge. Most of the blockchain technology follow bitcoins infrastructure and use Proof of Work as a consensus algorithm. To keep the system live it will need computational power. Mining will require you to solve complex equations using your computer. So, when you start mining, your PC will take more and more electricity to overcome this situation. At present, miners are using 0.2 percent of the total electricity. If it keeps increasing then, miners will take more power than the world can provide by 2020. Thus, it now becomes one of the primary challenges of this network.

2.3 Motivation

In this digital world, one of the biggest concerns for public entities specially in voting system, is to know precisely the identity of the voters. There are many attempts in past decades to develop technology to determine accurately and certify their basics attributes like name, address, credit record, etch but like EVM, the issues remain the same because of the conventional system.

Nevertheless Electronic voting machines (EVM) have been adopted precautiouslly in the India over 90s period. However EVM are always a controversial topic over all the election as the vote count is not auditable by the public. Hence they do not gain the confidence to the general public. So this motivates us to propose a models to empower the E-voting system that will overcome most of the issues of conventional system and set a new trend to research in this direction for efficient, secured and verified platform.
Now the blockchain technology, if used for voting, It has the potential to transform the scenario because the technology itself is open both in terms of how it works and open-source implementation. It could enable voters to verify his/her vote and allow to audit the votes tallied, also counting wold be completely automatically without any human intervention which could eliminate any dispute or any claim that the election is rigged. Digital Identity has taken a significantly important role in this area and becoming as a crucial security measure in this interconnected environment. This research is a systematic mapping review with the aim of verifying and overcoming the issues of traditional system through Digital Identity on Blockchain technology implemented on a Ethereum blockchain network environment. Hence there is a need for some secured and verified approach to find the solution for E-voting platform. Digital Identity has taken a significantly important role in this area and becoming as a crucial security measure in this interconnected environment. This research

is a systematic mapping review with the aim of verifying and overcoming the issues of traditional system through Digital Identity on Blockchain technology implemented on a Ethereum blockchain network environment. Hence there is a need for some secured and verified approach to find the solution for E-voting platform.

2.4 Objectives of Our Research

Conventional voting system is very complex and time taking process that consumes a very large amount of fund and manpower which reduces its efficiency. The Blockchain enables to provide safe and secure way to organise a digitally verified platform to conduct an efficient voting system. In our submission we provide a basic architecture of blockchain enabled network that provide a smart way to conduct e-voting that overcome all the issues of conventional system with higher efficiency and security.

The main objective of the proposed research work is to design efficient E-voting platform for secured and efficient solution for traditional voting system that set a new pathway in a direction towards the modern architecture based on blockchain technology. Here we are going to propose a simple basic model using Ethereum blockhain network.

2.4.1 The objective of our research also includes:

1. Study of different appllication based on blockchain network and challenges in efficiency and security issues.
2. Study of some existing modern voting system and e-voting system like EVM's issues and its downside.

3. Study of Ethereum blockchain network to test a prototype of e-voting based on it.
4. To study the existing models and to develop new models to improvise the performance.
5. Propose a framework for decentralised E-voting platform using Ethereum blockchain network.
6. To implement the proposed models and find out the overall performance of the decentralised network.
7. Comparison of the simulation results with existing models to show the effectiveness of the ideas.
8. Comparative analysis of the proposed models.

2.5 Organization of The Thesis

This thesis is organized into the following chapters.

- **Chapter 1:** Introduction of the blockchain network and the downside of the traditional voting system in India.
- **Chapter 2:** Application of blockchain network that are transforming society and its limitations are discussed in this chapter including motivation and objective of our research work.
- **Chapter 3:**Literature Review, contains the referance of the papers that has been used for research work and implementation.
- **Chapter 4:**Discuss the basic concept about Ethereum network and its benefits and downside including dependencies and implementation process.
- **Chapter 5:** Consists implementation details and testing result that describes a comparative analysis of the proposed models.
- **Chapter 6:**Deals with comprehensive summary and conclusions of the approaches that have been developed during the course of investigation.

Chapter 3

Literature Review

- Micha Pawlaka, Aneta Poniszewska-Marandaa, Institute of Information Technology, Lodz University of Technology, Lodz, Poland, Natalia Kryvinskab, Towards the intelligent agents for blockchain e-voting system.
- Mrs. Harsha V. Patil1, Assistant Professor, Dept. of Computer Science, Dr. D .Y. Patil ACS College, Pune, India, "A Study on Decentralized E-Voting System Using Blockchain Technology".
- Somnath Panja, Bimal Kumar Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain".
- Raja Naeem Akram, and Konstantinos Markantonakis, Royal Holloway, University of London, United Kingdom, " An E-Voting Protocol with Decentralisation and Voter Privacy".
- Andrew Barnes, Christopher Brake and Thomas Perry, Team Plymouth Pioneers Plymouth University, "Digital Voting with the use of Blockchain Technology".
- Gaby G. Dagher, Boise State University, Boise, Idaho, U.S.A, "Secure Voting System using Ethereums Blockchain".
- Dr.Rekha.B.Venkatapur, Prabhu B, Navya A, Roopini R, Sai Niranjan A S, at K S Institute of Technology Bengaluru, India,

"Electronic Voting Machine Based On Blockchain Technology and Aadhar Verification".

- Massimo Di Pierro in the School of Computing at DePaul University What Is the Blockchain? Published in Computing in Science Engineering (Volume: 19, Issue: 5, 2017).
- Michael Mainelli And Alistair Milne, SWIFT INSTITUTE,WORKING PAPER NO. 2015-007,"THE IMPACT AND POTENTIAL OF BLOCKCHAIN ON THE SECURITIES TRANSACTION LIFE-CYCLE".

Chapter 4

Methodology of the application

Et cum codice Ethereum blockchain ipsum facere sinit Ethereum Rectum Apparatus (EVM) acri et ad blockchain contractum.

4.1 Ethereum

It is an open software platform which is based on blockchain technology that enables the developers to build and execute decentralized applications. It enable the developers to build and deploy decentralized applications over this blockchain powered network.

4.2 Differences Between Ethereum and Bitcoin

Ethereum is a distributed public blockchain network. There are some significant technical differences between the them, the most important differences in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that allows online Bitcoin payment transactions,the Bitcoin blockchain is used for tracking ownership of digital currency (bitcoins),Whereas the Ethereum blockchain focuses on running and executing the programme code for any decentralized application. In the Ethereum blockchain miners work to earn Ether, Ether is basi14 cally used by application developers to pay for transaction fees and

services on the Ethereum network. In opus ad Ethereum blockchain fossoribus earn Athar et Athar est basically usus developers per applicationem ad rem reddere in Ethereum fees et officia network.

Another type of token which is used to pay miners fees for including transactions in their block, it is called "gas", and each and every smart contract deployment requires a certain amount of "Gas fee" i.e to be sent along with it to entice miners to put it in the blockchain.

4.3 The characteristics of a decentralized Ethereum Blockchain Network

Immutable No any third party make changes to data as it is decentralise and any temper with information would be detected.

Corruption and tamper proof It makes censorship impossible.

Secure Contains no loophole as it has no any central point of failure, here applications are strongly protected against hacking attacks, fraudulent activities or any tempering with data would be detected.

Zero downtime It has zero downtime since apps never go down and can't be shutdown.

4.4 Downside of decentralized Ethereum applications

Decentralized applications arent fully secured. Since smart contracts are code which is basically written by coders, So the smart contracts would be as good as the coders who write them. Code bugs can lead to adverse actions being taken. If a mistake in the code gets detected, there is no any efficient way to stopp the attack, the only option we have is to obtaining a network consensus and rewriting the underlying code. This goes against the essence of the blockchain which is meant to be immutable. Also, any action taken by a central

party would raise serious questions about the future of decentralized nature of an application.

4.5 Smart contracts

Smart code are the set of codes and agreement that directly control the transfer of digital assets between nodes or computer under certain condition.These contracts are are generally stored on blockchain network. They are very complex and having a huge potential that goes beyond the level of simple transaction. As of now this is not very popular among techie but in future it has potential to disintregate the many existing fields and financial industries.

4.6 Implementation of work

Here is a demonstration of the voting application that we are implementing. A client-side decentralised application that will communicate to our smart contract on the blockchain. This client-side application will have a table of candidates i.e contesting election that lists each candidates id, name, and vote count. There will be a form where we can cast a vote for our desired candidate. Here It also shows the account were connected to the blockchain with under your account. In order to build our dApp, we need a few dependencies

4.7 Installing Dependencies

4.7.1 Ganache

Ganache is a personal blockchain, which is a confined development blockchain network that can be used to copy the quality feature of a public blockchain for Ethereum development. It is available on Windows, Mac, and Linux as as a desktop application and a command line tool. Node.JS Now that you have a private blockchain

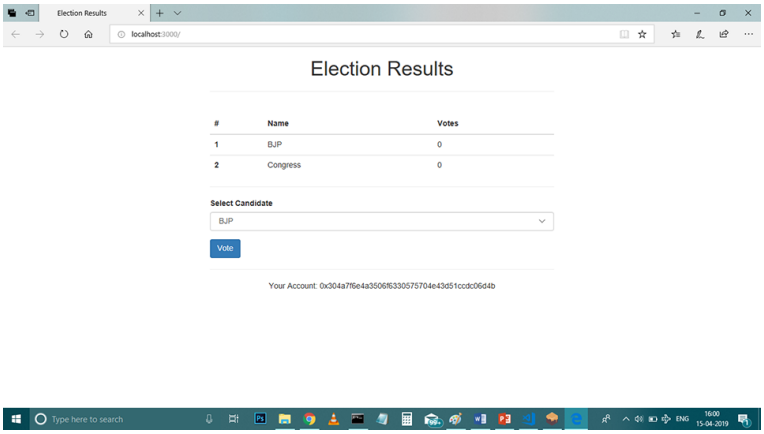

Figure 4.1: E-Voting Homepage

running, it require to configure the environment for producing smart contracts. It is the very first dependency that we will need is Node Package Manager, or NPM, which comes along with Node.js.

4.7.2 Truffle Framework

Truffle Framework, which provides a suite of tools for developing Ethereum smart contacts with the Solidity programming language.

The functionality of the Truffle Framework:

Managing Smart Contract - Here we code smart contracts with the Solidity programming language and then after we will compile it that will generate the bytecode that is going to run on the Ethereum Virtal Machine (EVM).

Automated Testing - It write tests in anticipation of our smart contracts to ensure that it behave the way we want them to behave. Deployment and Migrations - It is responsible for writing scripts to migrate and deploy the smart contracts to public Ethereum blockchain network. Development Console - Responsible for interacting to the smart contracts inside a JavaScript runtime environment along with the Truffle Console. We can also connect to blockchain network that weve specified within our network setup. Script Runner - Script Runner Write precedent scripts used to run

against the public blockchain network with JavaScript. Client Side Development - Client Side Development will setup the truffle project. It will host the client side applications that is going to communicate with smart contracts that would be executed to the blockchain.

4.7.3 Metamask Ethereum Wallet

In order to use the blockchain, we must connect to the blockchain network. We have to install a browser extension for executing Ethereum blockchain network. After this we will be able to connect to our local Ethereum blockchain network with our metamask personal account, that will directly interact with the smart contract.

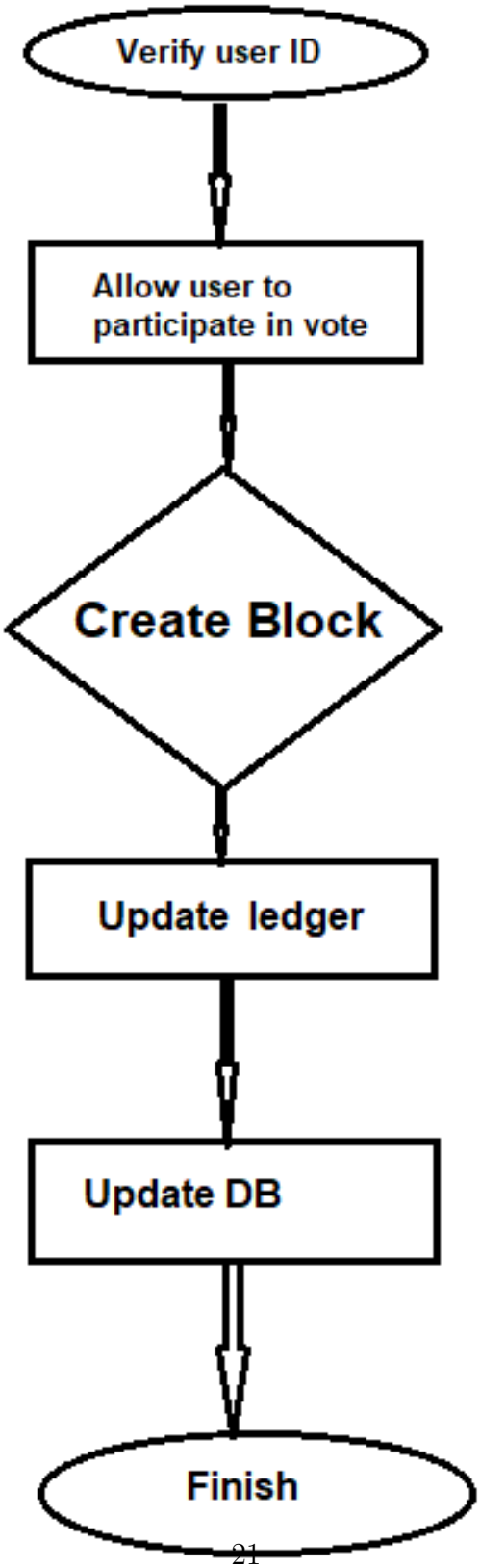

Figure 4.2: Flow Diagram

Chapter 5

Implementation

5.1 Ganache Personal Blockchain

Ganache is a kind of a personal blockchain, It is a local development blockchain network, that can be used to copy the characteristics of a distributed public blockchain for Ethereum development. It will allow us to execute our work, after developing decentralised applications, we can proceed for the tests.

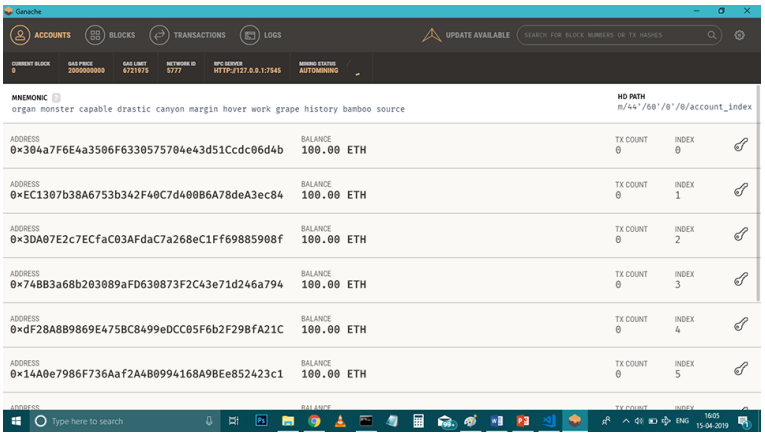

Figure 5.1: Ganache Homepage

Now in this personal blockchain running network,We can observe in the above figure in details about the server Ganache is running,each account has been credited with 100 ether by default, along with a list of accounts connected to the network. Each and every account

has a unique address and a private key that will serve as a distinct identifier for each and every voters in the election. This is a big time saver, If we would create any personal blockchain network from the very begining, or develop any type of application on a test network, then we should have to build all the accounts manually and credit each account with ether. Now lets create a project directory for our decentralised application in the command line like this: mkdir election cd election Now if we want to run fast, then in that case we go with a Truffle box. We will use the Pet Shop box for this project. Now the next step is from within the project directory, install the pet shop box from the command line terminal as shown below:

- truffle unbox pet-shop

Pet shop box contains the following items:-

Smart contract directory: Here all smart contacts code resides,also the migration contract will handle the movement to across the network.

Migrations directory: Relocated files resides here. These migrations are same to other web frameworks that needs migrations to transform the condition of a database. Whenever we execute smart contracts to the blockchain, we are updating the blockchains condition, and therefore it require migration

Node modules directory: It is the hub for the maximum Node dependencies.

Src directory: Here well implement our tests for our smart contracts

Test directory: Here we'll implement our tests for our smart contracts.

Truffle.js file: Contains the main configuration and setup file for implementing the Truffle project

5.2 Writing our smart contract

- **contracts/Election.sol**

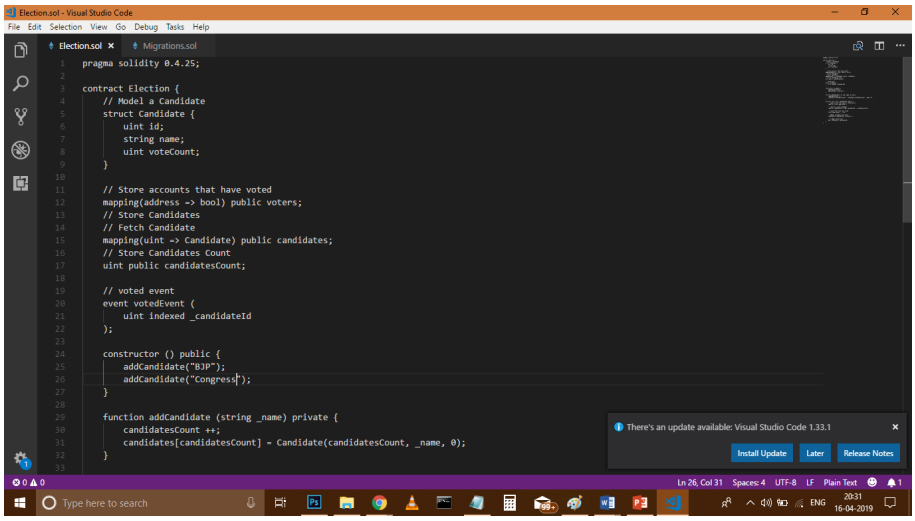

Figure 5.2: election homepage

- **Client-Side Application**

5.3 Result Of The Implementation and Testing

- The code that run over the network is unchangable, basically it can not be changed. Incase if the code contains any errors, we must disable it and develop a corrected version.

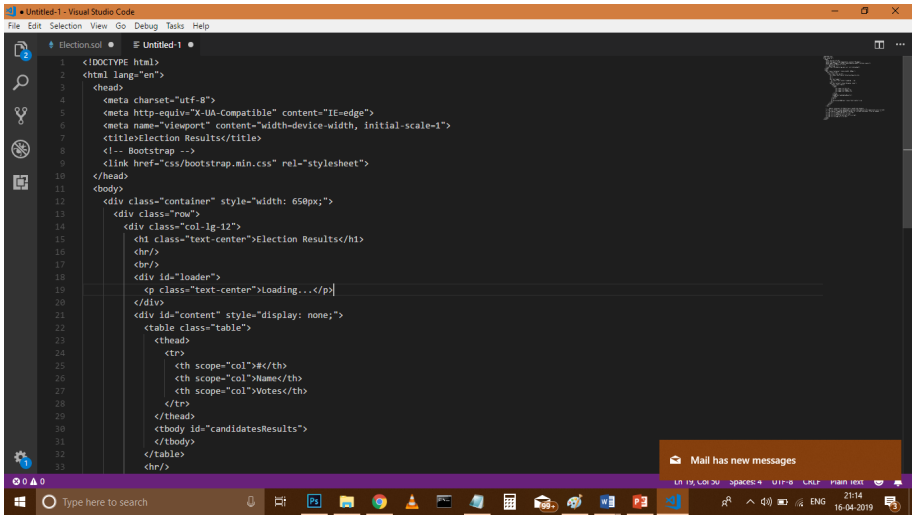

Figure 5.3: client side -index.html

- Whenever the deployment of the contract has been done, it usually cost a "Gas fee" because it creates a transaction and writes data over the blockchain network. so it cost Ether.
- If any of the functions that written to the Ethereum blockchain network consists of any type of bugs, the account that calling this function could potentially waste their own Ether amount, and it may not respond the as expected.

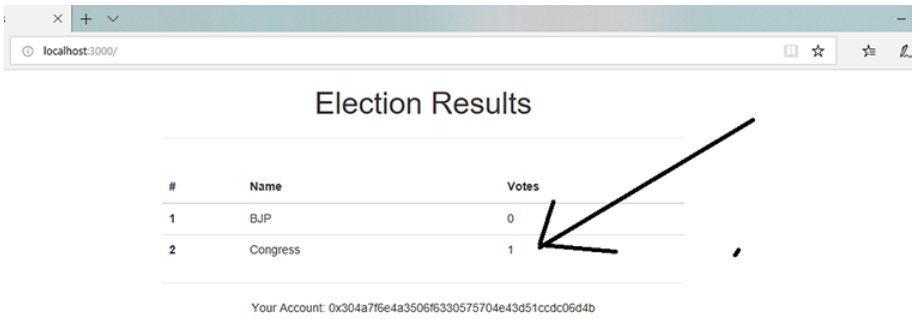

Figure 5.4: Now your front-end application should look like this:

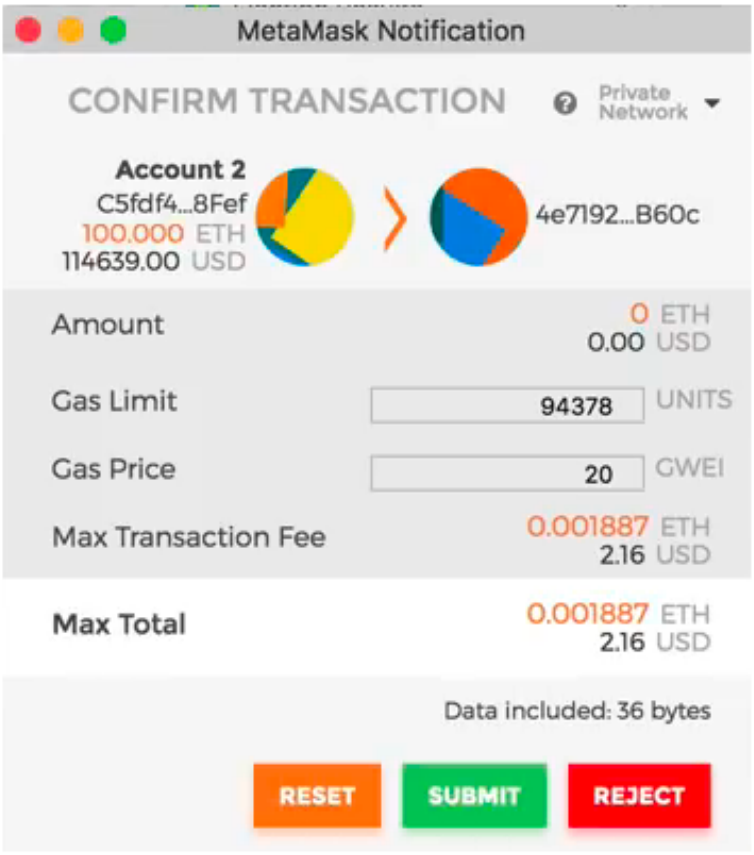

Figure 5.5: result

- When we call the voting function. Once submited then we will see Metamask confirmation pop up like this:
- Now, we can vote on our client-side application, and watch the votes recorded in real time, it might take a few seconds for the event to trigger.
- Here we have successfully implemented a full stack decentralized application on the Ethereum blockchain.

Chapter 6

Conclusion

Today the blockchain technology is currently in a nascent state. There havent been enough distributed decentralised platform technology and blockchain based applications to exactly evaluate whether this technology is superior to current voting systems neither any full implementation of e-voting platform for a election has occurred yet anywhere in the world. However, We could say that e-voting has a future in elections and could overcome traditional voting issues, also Political violence related to elections has been very common in most of the developing countries. E-voting can ensure security, transparency and reduce the electoral violence and other related issues or downside. We could say that this platform can also produce more mathematically accurate election results that could be verified anytime. E-voting doesnt require management from a central authority, voting related expenditure will decrease sharply which can be used in other fields for development works. Hence, there is more work and research yet to be done for the development of this technology that could transform the world and this just the beginning.

Bibliography

[1] Rourab Paul, Suman Sau, Paresh Baidya, Satyabrata Maity, Sudhindu Bikash Mandal, Krishanu Maity, IoT based Secure Smart City Architecture using Blockchain.

[2] Gregory from Dapp University, The Ultimate Ethereum Dapp Tutorial .

[3] J. Demuro, Here Are the 10 Sectors That Blockchain Will Disrupt Forever, TechRadar Pro, 16 Jan. 2018; https://www.techradar.com/news /here-are-the-10-sectors-that -blockchain-will-disrupt-forever.

[4] B. Dickson, Blockchain Tech Could Fight Voter Fraudand These Countries Are Testing It, VentureBeat, 22 Oct. 2016; https://venturebeat .com/2016/10/22/blockchain -tech-could-fight-voter-fraud-and -these-countries-are-testing-it.

[5] G. Prico, Sierra Leone Pilots Blockchain-Based Voting for Political Elections, 22 Mar. 2018;

[6] Massimo Di Pierro in the School of Computing at DePaul University What Is the Blockchain? Published in Computing in Science Engineering (Volume: 19, Issue: 5, 2017