Savitribai Phule Pune University

Government College of Engineering and Research, Awasari

Manchar, Tal. Ambegaon, Pune – 412405.

A REPORT

ON

Blockchain Voting Dapp

B.E. (COMPUTER)

SUBMITTED BY

Shrishailyam Patil (18121051)

Vaishakh Autade(18121022)

Abhishek Waghmare(18121001)

UNDER THE GUIDANCE OF

Dr.S.U.Ghumbare

(Academic Year: 2021-2022)

Savitribai Phule Pune University

Government College of Engineering and Research, Awasari

Manchar, Tal. Ambegaon, Pune – 412405.

DEPARTMENT OF COMPUTER ENGINEERING

Certificate

This is to certify that project entitled

Blockchain Voting Dapp

has been completed by

Shrishailyam Patil(18121051)

Vaishakh Autade (18121022)

Abhishek Waghmare(18121001)

of BE COMP in the Semester - VIII of academic year 2021-2022 in partial fulfillment of the Final year of Bachelor degree in ”Computer Engineering” as prescribed by the Savitribai Phule Pune University.

Dr.S.U.Ghumbare
Project Guide

Dr.S.U.Ghumbre
H.O.D

ACKNOWLEDGEMENT

It gives me great pleasure and satisfaction in presenting this project on "Blockchain voting Dapp".

I would like to express my deep sense of gratitude towards **Dr.S.U. Ghumbare** for guiding us throughout the project.

I have furthermore to thank Computer Department HOD **Dr.S.U. Ghumbre** *who encouraged us to go ahead and gave continuous attention. I also want to thank other faculty members of the Computer Department for all their assistance and guidance for preparing report.*

I would like to thank all those, who have directly or indirectly helped me for the completion of the work during this project.

Shrishailyam Patil(18121051)
Vaishakh Autade (18121022)
Abhishek Waghmare (18121001)
B.E. Computer

Contents

List of Figures

Abstract

The systems that are currently present for voting are not trustworthy. Also, sometimes it is not feasible to implement regular voting methodology, because, as we seen issues faced by the people during corona time. Our voting system developed by using blockchain which is trustworthy and easy to use for any type(literacy level) of people.

The data or the information of every person is stored with hash key, that makes it more secure and also, our system is decentralised that makes it unique from other conventional methodology or system. It is mainly based on Remix IDE, ROPSTEN test network, etc. The decentralisation and trust are key factors while developing this system. Our aim is to provide easy to use and feasible as well as trustworthy system. In this system, we are mainly focusing on blockchain compatibility with easy to use for people.

Chapter 1

Introduction

1.1 Web3

Web3 has become a catch-all term for the vision of new , better internet. At its core, Web3 uses blockchains, cryptocurrencies, and NFTs to give power back to the users in the form of ownership.

1.2 Blockchain

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchain are best known for their crucial role in cryptocurrency systems, such as bitcoin, for maintaining a secure and decentralised record of transactions.

The innovation with a blockchain is that it gurantees the fidelity and security of a record of data and generates fidelity and security of a record of data and generates without the need for a trusted third party.

One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain.

1.3 smart Contract

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

1.4 Solidity

Solidity is an object oriented programming language created specifically by the etherium network team for constructing and designing smart contracts on blockchain platforms.

It is used to create smart contracts that implement business logic and generates a chain of transaction records in the blockchain system.

It acts as a tool for creating machine-level code and compiling it on the etherium virtual machine(EVM).

It has a lot of similarities with C and C++ and is pretty simple to learn and understand. For example, a ”main” in C is equivalent to a ”contract” in solidity.

1.5 Decentralised App

Decentralised applications also known as ”dapps” are digital applications that run on a blockchain network of computers instead of relying on a single computer. Because, dApps are decentralised, they are free from the control and interference of a single authority.

1.6 Metamask

Metamask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralised applications.

1.7 ROPSTEN Ethereum testnet

Ropsten Ethereum (also known as ”Ethereum testnet”) is an ethereum test network that allows for blockchain development testing before development testing before deployment on Mainnet, the main ethereum network.

1.8 Electronic Voting Machine

Electronic voting is the standard means of conducting elections using Electronic voting machines, sometimes called "EVMs" in india.

1.9 Ballot System

In the simplest elections, a ballot may be a simple scrap of paper on which each voter writes in the name of a candidate, but government elections use pre-printed ballots to protect the secrecy of votes. The voter casts their ballot in a box at a polling station.

1.10 Blockchain and Related terms

1.10.1 Encryption

In the IT world, encrypting information consists of hiding it in such a way that it can only be interpreted if the user has a password or code. It is a technique that allow users to protect the exchange of data and in which the processes are used more secure.

1.10.2 Cryptocoin or Cryptocurrency

Just like cash money, cryptocurrency is a means of exchange, but in this case, a digital one. The first cryptocurrency to begin operating was bitcoin, in 2009, after satoshi nakamoto established the basis of system.

1.10.3 Etherium

Etherium is a decentralised platform that enables the creation of ”smart contracts”; some have dubbed it a ”decentralised supercomputer”.

1.10.4 Nodes

The nodes are the computers that form part of the blockchain network.

1.10.5 Token

The tokens are units of value that can be acquired through blockchain, and are also used to acquire goods and services.

1.10.6 Hash

The groups of blocks with blockchain miners are charged with must be validated by the system. To do this, the miners must find a password or digital fingerprint that identifies them. This password is called a hash. It is unique, unrepeatable and cannot be modified.

1.11 Account Wallet

Blockchain wallet is also known as the name of a specific wallet provided by the company blockchain. This is an E-wallet that allows individuals to store and transfer cryptocurrencies. Blockchain wallet users can manage their balances of bitcoin, Ether and other crypto assets.

1.11.1 Private Key

Private key is a secret number that is used in cryptocurrency, similar to a password. In cryptocurrency, private keys are also used to sign transactions and prove ownership of a blockchain address.

1.11.2 Public Key

A public key allows you to receive cryptocurrency transactions. It's a cryptographic code that is paired to a private key. While anyone can send transactions to the public key, you need the private key to "unlock" them and prove that you are the owner of the cryptocurrency received in this transaction.

1.11.3 Miners

Bitcoin mining is the process by which bitcoin transactions are validated digitally on the bitcoin network and added to the blockchain ledger. It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralised blockchain ledger.

Chapter 2

Literature Review

In ancient greece, citizens used pieces of broken pottery to scrach in the name of candidate in the procedures of ostracism. The first use of paper ballots to conduct an election appears to have been in Rome in 139 BC, following the introduction of the lex Gabinia tabellaria.[1][2]

In ancient india, around 920 AD, in tamil nadu, palm leaves were used for village assembly elections. The palm leaves with candidate names were put inside a mud pot for counting. This was called kudavolai system.

The first use of paper ballots in america was in 1629 within the massachusetts bay colony to select a pastor for the salem church. Paper ballots were pieces of paper marked and supplied by voters.

A ballot is a device used to cast votes in the election and may be found as a piece of paper or small ball used in secret voting. It was originally a small ball used to record decisions made by voters initially around the 16th century.

Due to some problems and flaws, electronic voting machine comes into the picture in the 1990s. Electronic voting is the standard means of conducting elections using electronic voting machines, sometimes called "EVM" in india. The use of EVM and electronic voting was developed and tested by the state-owned electronics corporation of india and bharat electronics in the 1990s.[3]

They were introduced in indian elections between 1998 and 2001 in a phased manner prior to the introduction of electronic voting, india used paper ballots and manual counting. The paper ballots method was widely criticised because of fradulent voting and booth capturing, where party loyalists captured booths and stuffed with them with pre-filled fake ballots.

In recent elections, various opposition parties have alleged faulty EVMs after they failed to defeat the incumbent. After rulings of delhi high court, the supreme court of india in 2011 directed the election commision to include a paper trail as well as to help confirm the realiable operation of EVMs. The elction commission developed EVMs with voter-verified paper audit trail (VVPAT) system between 2012 and 2013. The election commission of india has acted under this order and deployed VVPAT verification for 20,625 EVMs in the 2019 indian general election.[3]

We can talk about, online voting in ontario, canada. The features in online voting as follows :

2.0.1 Secure Authentication:

Voters only gain access to their ballot after entering their credentials are authentication key on a secure login page.

2.0.2 User Interface:

Easy to use portal to help end users manage votes, manage votes eligibility and validate configurations prior to the vote.

Online voting platform assures that voters can vote with the strichest of confidentiality and security of measures in place 24/7.

In india, the government is considering proposals for linking Aadhar with the electoral rolls to check fradulent voting and granting of online voting to indians working abroad. The government is looking for to check double names in electoral rolls and fradulent voting and ensure a clean voting process through online voting.[4][5][6]

Chapter 3

Research Gaps and Problem Statement

3.1 Research Gaps

In references, the previous and current voting methodologies sometimes lead to political pressure, not feasible, trust issues, not convenient for old people, not easy to use, not good at everytime(Corona pandemic), etc. Here, our system is easy to use, trustworthy (blockchain used), convenient and many more.

3.2 Problem statement

In traditional voting, there are number of factors that make rigging in the whole electoral process such as, fake voters and involvement of outside sources and also other problems like time consumption, cost budget problems, etc.

Our system is authentic, reliable, time maintaining, verification, budget saving and trusty as well as decentralised system.

Chapter 4

Proposed Methodology/ Solution

In the current situation, we are using EVM (Electronic voting machine) system for election. But, we can't rely on one source of election i.e. offline mode of election. Now, we have to upgrade ourselves and to look for online election mode as well. Let us, discuss some cases like in the corona time, it is difficult to vote in the offline mode for almost every person.Also, in the normal situation, it is not feasible for old people to vote. In disaster situation we can't go with the offline mode. Also, there are people who are living abroad for them it is not always feasible to come to the country and vote.

We can replace EVM (Electronic voting machine) and set our dApp in the computer present that will going to help us to make process smooth and seamless.

4.1 Offline methodology

In current situation, the offline process is carried out in this way, firstly person have to register their name to the paper at election center. The government created a ethereum wallet for each individual person associated with the private key to that particular user. Then, the ticket is provided to the user associated with the private key and after going at main stage of election commitee people(associated people) put ink on the finger of voter and then voter enter private key on the metamask and then the voter vote and select ”YES” on metamask for confirmation the transaction for vote. This is how offline methodology work.

Figure 4.1: Offline Voting

4.2 Online methodology

The government will create the form for the people who want to go with online voting mode. The Aadhar card number and all the related important information is mandatory to all the people to fill in the form. Then the private key will be sent on the Aadhar registered / associated mobile number on the election day.

Voter have to go on website and have to enter the private key on the metamask and have to vote for particular candidate. After that he can confirm the transaction for vote. The voter's voting is noted on blockchain.

Figure 4.2: Online Voting

Chapter 5

Experimental Setup

5.1 Hardware requirement

- Intel core i3 11th gen
- 64 bit OS
- Windows or linux
- 8GB RAM

5.2 Software requirement

- Truffle :- Truffle is a world class development environment, testing framework and asset pipeline for blockchains using the ethereum virtual machine(EVM).
- Ganache :- Ganache is a personal blockchain for rapid Ethereum and corda distributed application development.
- Node :- Nodes are the computers that form part of the blockchain

network.

- Metamask Legacy :- It gives supports decrypted of modules of old web3.eth provider.
- Chai and Mocha testing Module :- These are the modules used for testing smart contract functions.
- ROPSTEN Testnet :- Ropsten Ethereum (also known as ”Ethereum testnet”) is an ethereum test network that allows for blockchain development testing before development testing before deployment on Mainnet, the main ethereum network.
- Etherscan :- Etherscan is a block explorer and analytics Platform for Ethereum, a decentralised smart contract platform.

Chapter 6

Results and Discussion

6.1 Advantages

- Electronic voting machine(EVM) can be tweaked to exchange to other candidate this can be prevented using our dapp blockchain system.

- In ballot system, The oragnizer person or main person can cheat in counting the votes and this will lead to unfair election. Using our dapp blockchain system we can prevent this.

- There are chances of system getting hacked and this lead to unfair election and our decentralised system can help us to prevent this.

- The traditional system is costly and our blockchain helping us to reduce the cost for the election.

- Our blockchain system reduced the use of paper as compared to traditional election system.

- Our blockchain sytem is more efficient than traditional methodology.
- Our blockchain system is transparent and accountability to proving the person is voted or not.

6.2 Discussion about features

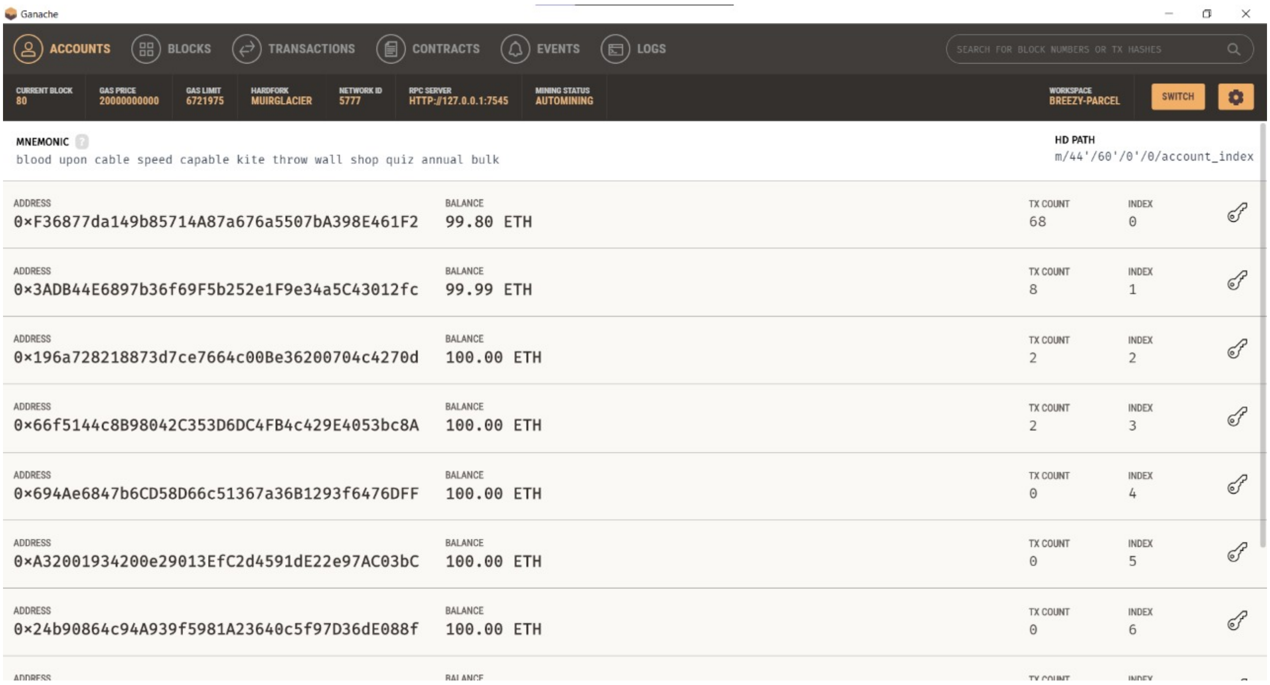
This project is divided into two prototypes, the one dApp prototype is deployed on local blockchain and other one is deployed on live blockchain.

6.2.1 Local Blockchain

This dApp smart contract is deployed on local blockchain by using special tool. In this, we are using truffle provides development and testing framework for the blockchain technology. We are also using ”ganache” a tool from truffle suite and also using testing modules chai and mocha which are embedded in truffle.

We joined ganache to metamask which is running on local server at port 7545 having chain Id 1377. After joining, we can import accounts to metamask.

We use boilerplate code name ”Pet Shop” from truffle boxes as a base code. We wrote smart contract in solidity language for voting functions in ”Election.sol”.Then, we deploy the smart contract on



CURRENT BLOCK 80 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE BREEZY-PARCEL

MNEMONIC
blood upon cable speed capable kite throw wall shop quiz annual bulk

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×F36877da149b85714A87a676a5507bA398E461F2	99.80 ETH	68	0
0×3ADB44E6897b36f69F5b252e1F9e34a5C43012fc	99.99 ETH	8	1
0×196a728218873d7ce7664c00Be36200704c4270d	100.00 ETH	2	2
0×66f5144c8B98042C353D6DC4FB4c429E4053bc8A	100.00 ETH	2	3
0×694Ae6847b6CD58D66c51367a36B1293f6476DFF	100.00 ETH	0	4
0×A32001934200e29013EfC2d4591dE22e97AC03bC	100.00 ETH	0	5
0×24b90864c94A939f5981A23640c5f97D36dE088f	100.00 ETH	0	6

Figure 6.1: Ganache UI

local blockchain by using following command:

truffle migrate

You can check details and retrieve data from smart contract instance by using following command:

truffle console

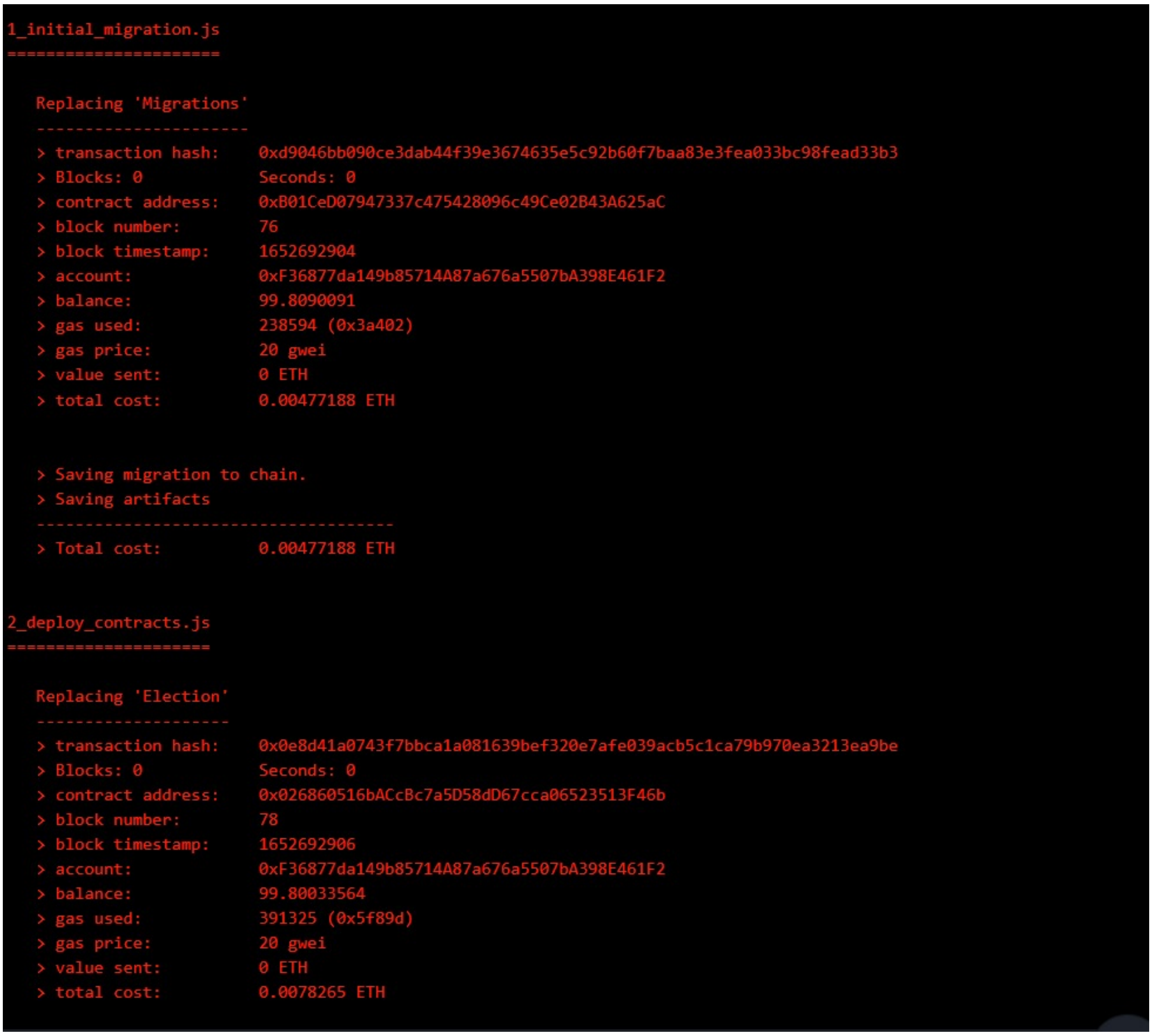
Also, we have written test cases with the help of modules like chai and mocha and we can run the test by following command:

truffle test

The frontend part is developed using technologies like html, Css, Javascript. To support old web3.eth provider functions we have added "metamask legacy" module.

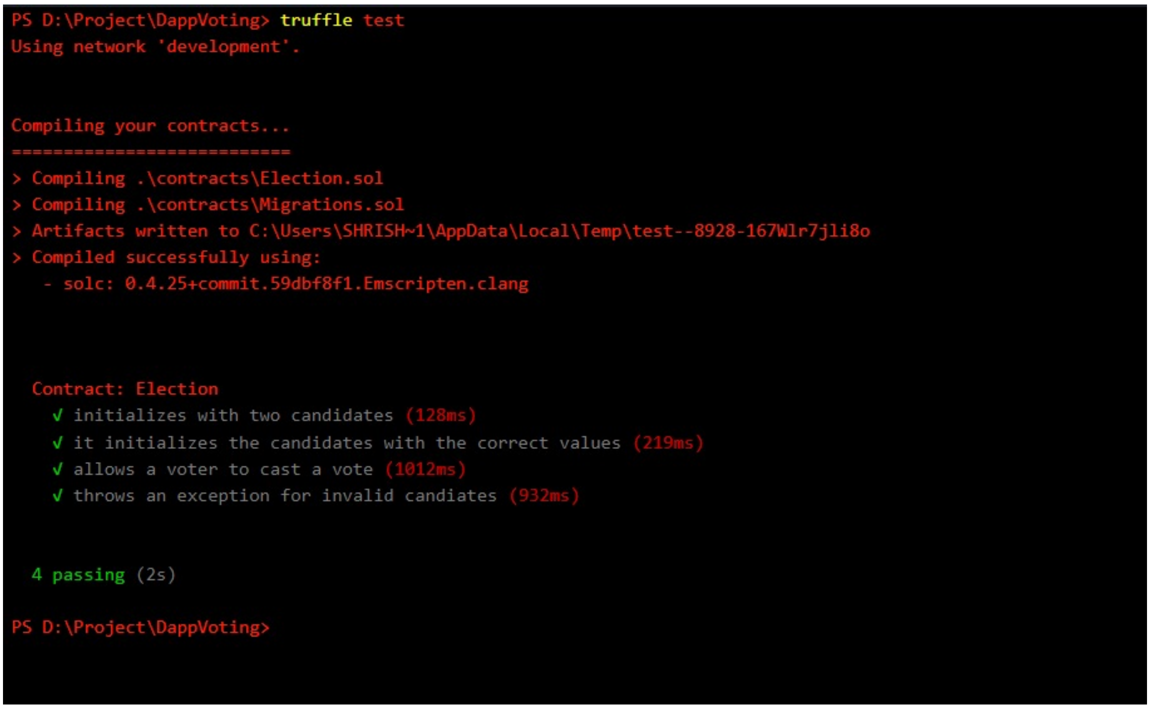
Working

- Firstly, User will open the website.



```
1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0xd9046bb090ce3dab44f39e3674635e5c92b60f7baa83e3fea033bc98fead33b3
   > Blocks: 0            Seconds: 0
   > contract address:    0xB01CeD07947337c475428096c49Ce02B43A625aC
   > block number:        76
   > block timestamp:     1652692904
   > account:             0xF36877da149b85714A87a676a5507bA398E461F2
   > balance:             99.8090091
   > gas used:            238594 (0x3a402)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00477188 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00477188 ETH


2_deploy_contracts.js
=====================

   Replacing 'Election'
   --------------------
   > transaction hash:    0x0e8d41a0743f7bbca1a081639bef320e7afe039acb5c1ca79b970ea3213ea9be
   > Blocks: 0            Seconds: 0
   > contract address:    0x026860516bACcBc7a5D58dD67cca06523513F46b
   > block number:        78
   > block timestamp:     1652692906
   > account:             0xF36877da149b85714A87a676a5507bA398E461F2
   > balance:             99.80033564
   > gas used:            391325 (0x5f89d)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0078265 ETH
```

Figure 6.2: Election Contract deployed



```
PS D:\Project\DappVoting> truffle test
Using network 'development'.


Compiling your contracts...
===========================
> Compiling .\contracts\Election.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\SHRISH~1\AppData\Local\Temp\test--8928-167Wlr7jli8o
> Compiled successfully using:
   - solc: 0.4.25+commit.59dbf8f1.Emscripten.clang



  Contract: Election
    √ initializes with two candidates (128ms)
    √ it initializes the candidates with the correct values (219ms)
    √ allows a voter to cast a vote (1012ms)
    √ throws an exception for invalid candiates (932ms)


  4 passing (2s)

PS D:\Project\DappVoting>
```

Figure 6.3: Testing

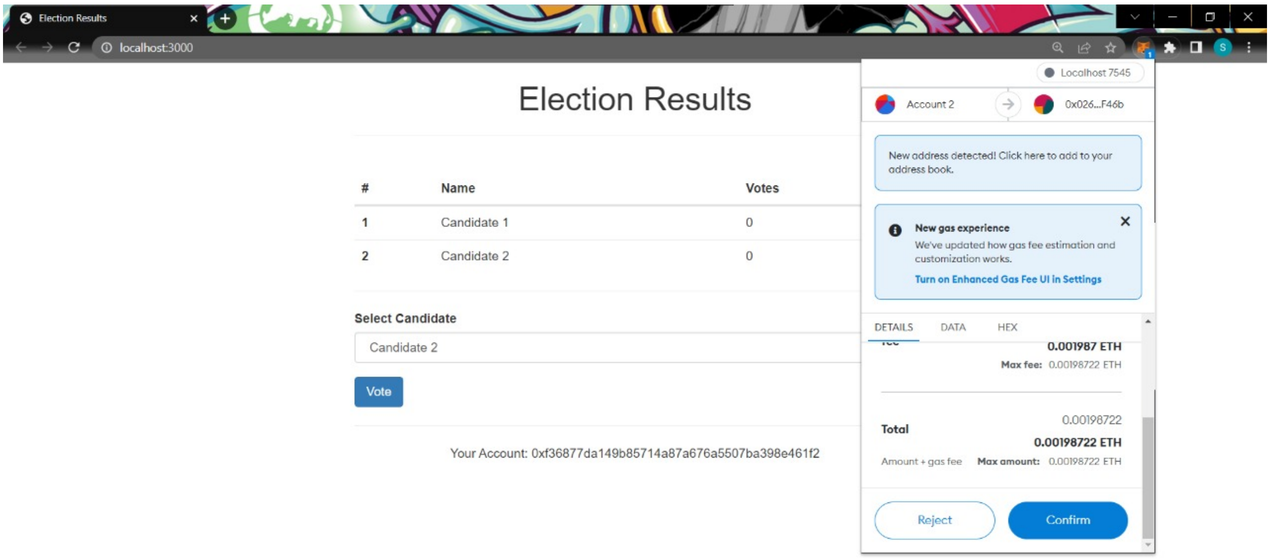
- The web3 function in smart contract will check if there is any web3 provider or metamask is present or not from user side.

- After detecting web3 will connect with metamask and the respective account address will be shown on the website.

- Then user will choose appropriate candidate name from drop-down and click the vote button.

- A metamask popup will be opened in which the details about the transition about voting will be present and two options accept and reject will be present. User must choose accept button to finalise the vote.

- Asynchronous function will send the data to a smart contract



Election Results

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	0

Select Candidate: Candidate 2

Your Account: 0xf36877da149b85714a87a676a5507ba398e461f2

New address detected! Click here to add to your address book.

New gas experience
We've updated how gas fee estimation and customization works.
Turn on Enhanced Gas Fee UI in Settings

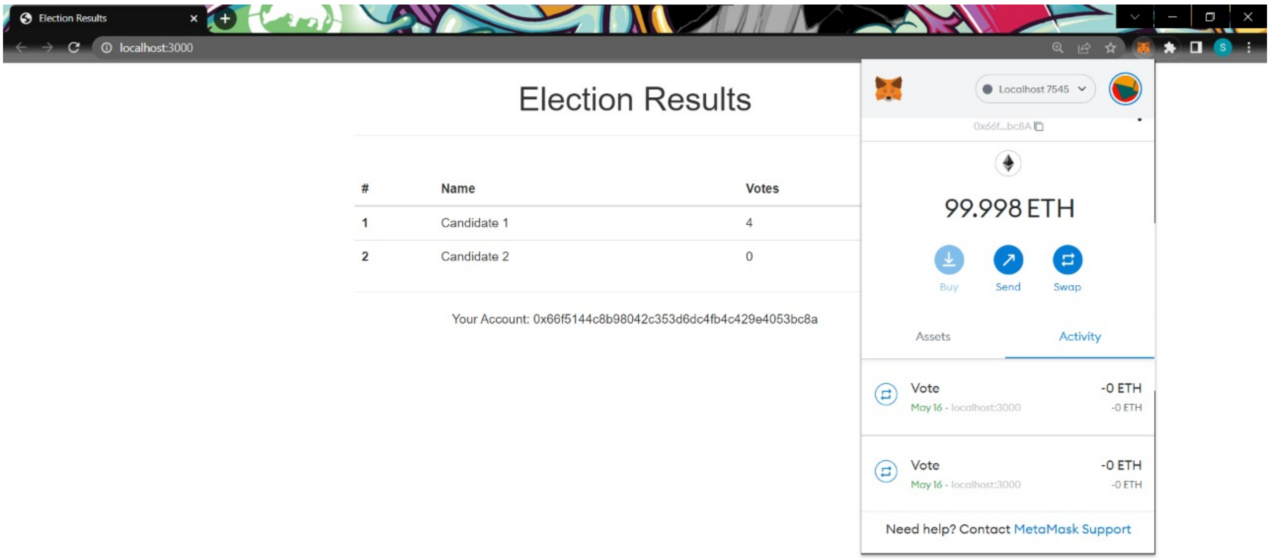
0.001987 ETH
Max fee: 0.00198722 ETH

Total 0.00198722
0.00198722 ETH
Amount + gas fee Max amount: 0.00198722 ETH

Figure 6.4: Voting process

function and the function will first check the address then if the address is already voted or not and if not voted it will increase the vote by 1 for respective candiadte.

- A event named voteEvent is triggered, that will check all the blocks data and return the data to javascript function.
- This will redirect to result page which shows the data from javascript function.
- As per the rule, every account can vote only once. So, even if after voting user refresh the webpage, the user will be stucked on result page only.



Election Results

#	Name	Votes
1	Candidate 1	4
2	Candidate 2	0

Your Account: 0x66f5144c8b98042c353d6dc4fb4c429e4053bc8a

Vote -0 ETH
May 16 · localhost:3000 -0 ETH

Vote -0 ETH
May 16 · localhost:3000 -0 ETH

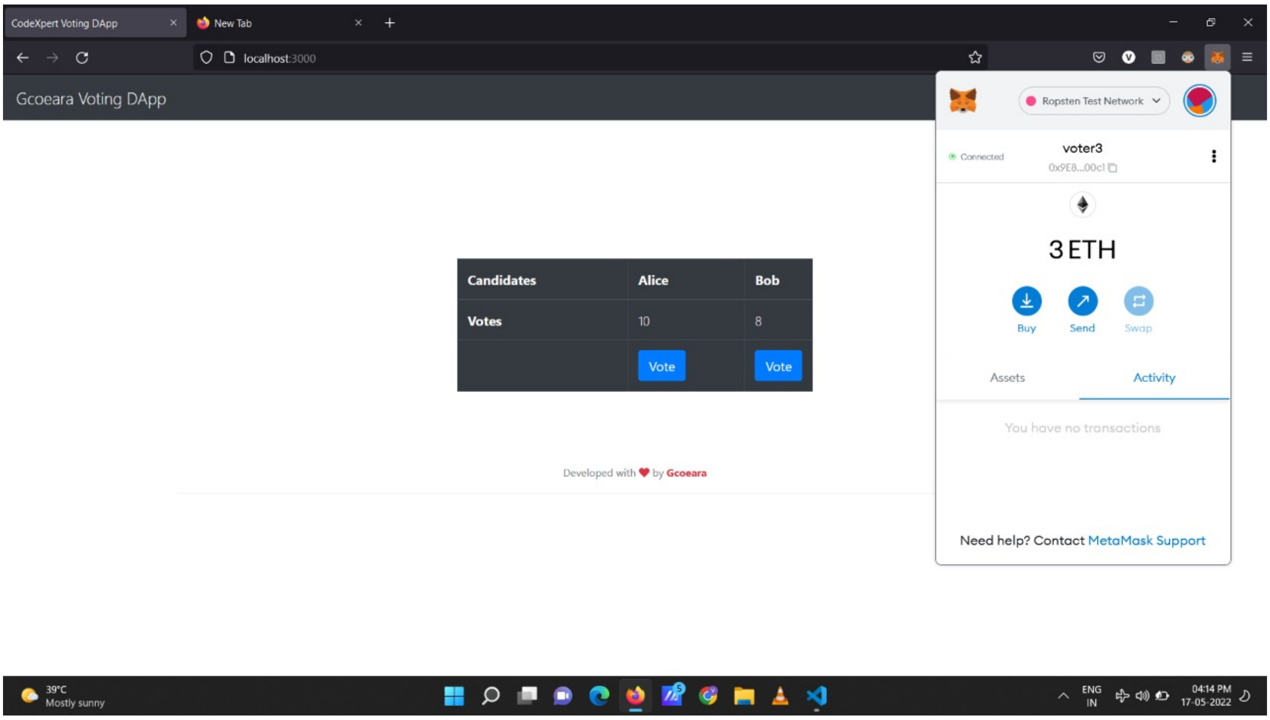
Figure 6.5: Election result

6.2.2 Live ROPSTEN Test network Blockchain

We wrote this smart contract on remix.ethereum.org and connected to our front-end which is hosted on localhost using ABIcode and smartContractAddress of smartContract.

Metamask is used to transact on Blockchain Network. Two extensions are used for transacting on blockchain network namely Metamask and Metamask legacy extension which supports transacting on current blockchain network and previous version. For connection we use contract.js and for voting home page voting.js.

In the backend, we used nodejs and to install dependencies we used npm also, install web3. In the front-end we used technologies like html, Css, Javascript, bootstrap. In the backend we use nodejs



Gcoeara Voting DApp

Candidates	Alice	Bob
Votes	10	8
	Vote	Vote

Developed with ❤ by Gcoeara

Ropsten Test Network

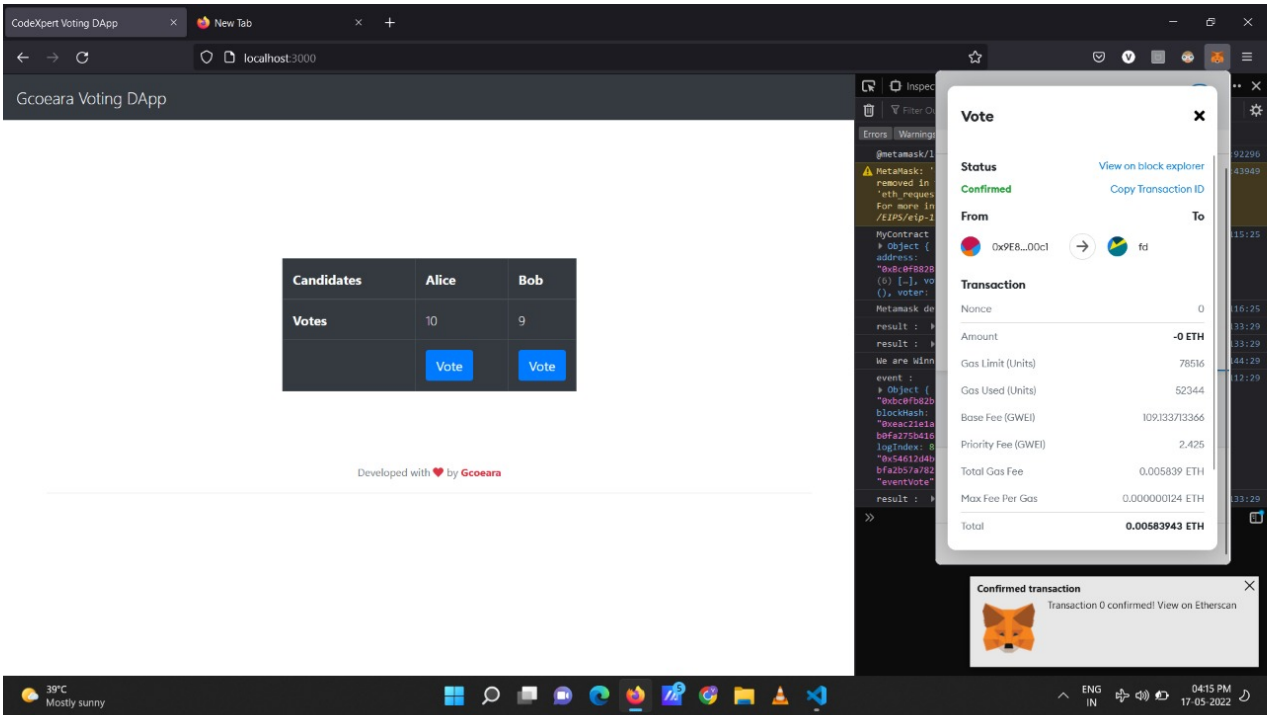
voter3
Connected
0x9E8...00c1

3 ETH

You have no transactions

Need help? Contact MetaMask Support

Figure 6.6: Initialization



Gcoeara Voting DApp

Candidates	Alice	Bob
Votes	10	9
	Vote	Vote

Developed with ❤ by Gcoeara

```
@metamask/l
MetaMask: '
removed in
'eth_reques
For more in
/EIPS/eip-1
MyContract
▸ Object {
address:
"0x8c0f882B
(6) [-], vo
(), voter:
Metamask de
result :
result :
We are Winn
event :
▸ Object {
"0xbc0fb82b
blockHash:
"0xeac21e1a
b0fa275b416
logIndex: 8
"0x54612d4b
bfa2b57a782
"eventVote"
result :
```

Vote

Status — View on block explorer
Confirmed — Copy Transaction ID

From 0x9E8...00c1 → **To** fd

Transaction

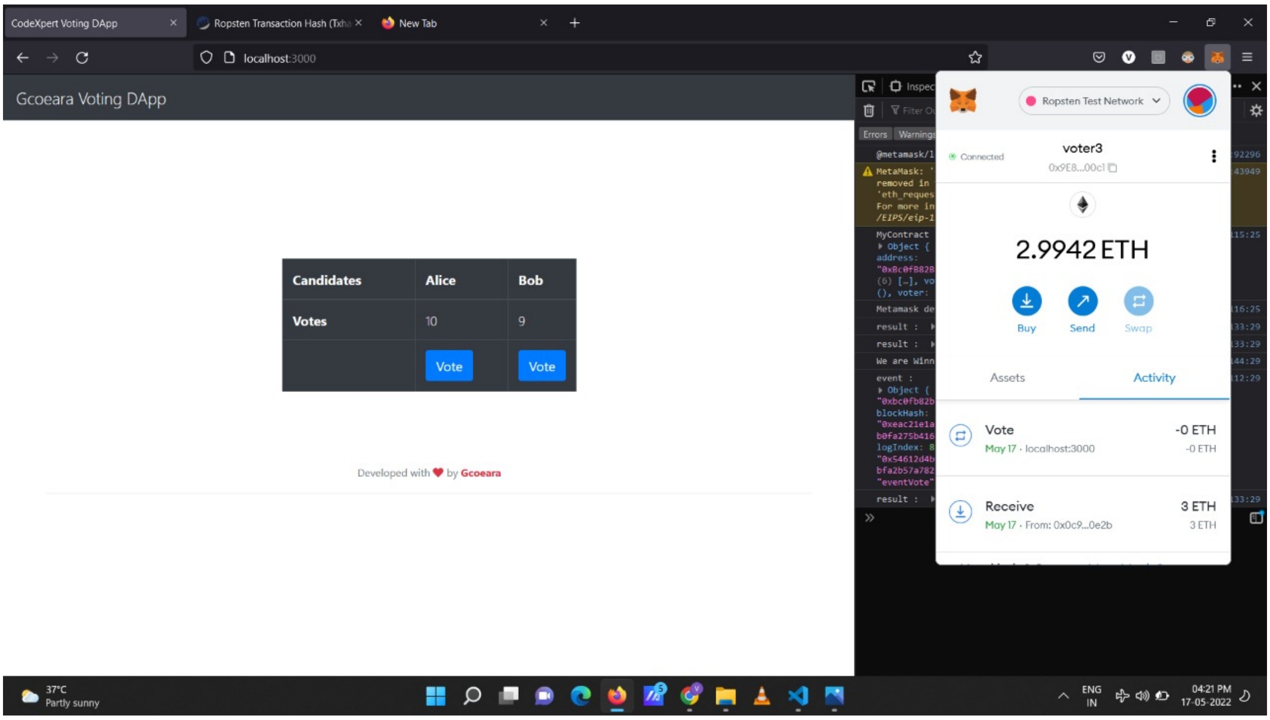
Nonce	0
Amount	-0 ETH
Gas Limit (Units)	78516
Gas Used (Units)	52344
Base Fee (GWEI)	109.133713366
Priority Fee (GWEI)	2.425
Total Gas Fee	0.005839 ETH
Max Fee Per Gas	0.000000124 ETH
Total	0.00583943 ETH

Confirmed transaction

Transaction 0 confirmed! View on Etherscan

Figure 6.7: Transaction

and to deploy our smart contract and transact vote on blockchain network we used ROPSTEN test network.



Candidates	Alice	Bob
Votes	10	9
	Vote	Vote

```
@metamask/l                 :92296
MetaMask: '                 :43949
removed in
'eth_reques
For more in
/EIPS/eip-1
MyContract                  :15:25
▸ Object {
address:
"0xBc0fB82B
(6) […], vo
(), voter:
Metamask de                 :16:25
result :  ▸                 :33:29
result :  ▸                 :33:29
We are Winn                 :44:29
event :                     :12:29
▸ Object {
"0xbc0fb82b
blockHash:
"0xeac21e1a
b0fa275b416
logIndex: 8
"0x54612d4b
bfa2b57a782
"eventVote"
result :  ▸                 :33:29
```

Figure 6.8: Voted

In figure 7.6, we created a new metamask account and top-up the metamask account with 3 ether, then, In figure 7.7, we vote to our candidate upon clicking vote metamask pop-up occurs asking us to confirm the same transaction and also checks if we have sufficient balance. After confirming the transaction, metamask transfers some part of ethereum from our account for the transaction upon completion of transaction which takes approximately 30 seconds, the transaction is completed and the vote is added to the respective candidate.

We can always go to ropsten.etherscan.io to verify our transaction and also look at any transaction occured on the candidate account or our account, Hence, making it secure process.

6.3 Future scope

- In future, in our system we can add face recognition facility for identification.
- In US, they use social security number(SSN) for person's identity during election that we can implement in future in india.
- We can automate some part of process in future, After Entering social security number(SSN), we can automatically implement the mapping of social security number and private key to login directly.
- We can also use for multiple candidate.

Chapter 7

Conclusion

Here, we can conclude that, we have made authentic, reliable, time maintaining, verification, budget saving, trusty, tamper proof, decentralised app for voting in election which makes smooth and seamless, elections fair, efficient and trustworthy.

Appendix A

Biblography

1] National Archives(US).Ballot system history from wikipedia. May 2022.

[2] Ballot Paper design: Evidence from an Experimental study at the 2009 Local Election. October 2015.

[3] Electronic Voting in India. From wikipedia. March 2022.

[4] Ontario, canada Online Voting.Professional Online voting services. From their Website. 2007-2022.

[5] Government considering to link Aadhar with electoral rolls, online voting for indians in abroad. statements from union law minister kiren Rijiju. Mar 2022.

[6] Complete guide to voting for non-resident indians. January 2019.