MAJOR PROJECT

REPORT

ON

Blockchain Voting App

Submitted by

Vipin Kumar Dinkar

03916404517

Under the supervision of

Dr. M. Bala Krishnan

Associate Professor

in partial fulfilment of the requirement for the award of degree of

MASTER OF COMPUTER APPLICATION

IN

SOFTWARE ENGINEERING

University School of Information, Communication & Technology,
Guru Gobind Singh Indraprastha University, New Delhi.
Jan-May, 2020

CERTIFICATE

This is to certify that the thesis entitled "Blockchain Voting App" is a bonafide record of independent project/research work done by me under the supervision of Dr. M. Bala Khrishnan And submitted to Guru Gobind Singh Indraprastha University in partial fulfillment for the award of the Degree of Masters of Computer Applications . I Certify the content of the thesis are original and free from Plagiarism.

Name and Signature of the student

(Vipin Kumar Dinkar 03916404517)

This is to certify that the thesis entitled "Blockchain Voting App" is a bonafide record Of independent project/research work done by “Vipin Kumar Dinkar” bearing enrollment number 03916404517 under my supervision.

Name and Signature of Supervisor

(Dr. M. Bala Khrishnan)

Associate Professor USICT

ACKNOWLEDGEMENT

During this project work, I came across a few such people who left a strong impression on me. I feel besieged to spell few names those were the source of inspiration behind this project work and their help and support made me to accomplish this demanding task.

First and foremost, with a profound sense of gratitude, I acknowledge the valuable scrupulous guidance rendered by my supervisor Dr. M. Bala Khrishnan who has not been just a guide but also an inspiring teacher,

an eminent academician and an incredible human being. It has been an honor for me to be his student. To me, he is not just the supervisor of my major project but instead I look upon him as an architect of my academic destiny.

I want to extend my special thanks to all my team mates who supported and helped me with their effort and other faculty members of University School Of Information and Communication Technology for their encouragement and guidance throughout the project work. I am also thankful to non-teaching staff and library staff of University School of Information and Communication Technology of for their help throughout this work. I wish to extend my very special thanks towards my family members for their continuous support and

encouragement during the project work. Last but not the least, I am thankful to God without whose grace all the wonderful people wouldn't have come into my life. Almighty God has always been the invisible divine force behind my accomplishments and I know that He will continue to do so forever.

(Vipin Kumar Dinkar)

Table of Contents

Abstract

We live in a country where we have democracy that's why we have a voting right. We can choose any candidate of our choice. In India we use EVM (Electronic Voting Machine) [4]
In place of paper. We thought that digitalizing the process of voting will help us in removing corruption and fraudulent activities and we were in a impression that it happened.

But in a demo [3] by APP (Aam Admi Party) in 2017 assembly, showed us that we are wrong. Evm are easily hackable hence, our voting right is used wrongly.

Here comes a new era of Decentralized networks, Cryptocurrency which ensures that no transaction can be hacked or modified since it goes thought all the nodes for verification.[13]
So why don't we use it as it provides security as the hash will require tremendous amount of time before we can manipulate it. The blockchain network as it is not owned by any single organization can be prone to 51% attack. Still the incentive is far greater than the outcoming.

Introduction

Blockchain

The blockchain is a like a immutable linked list which records every transaction happens.

The blocks are added to blockchain in a sequential and linear. The blockchain network have all the information from the origin (genesis) block to the latest block and can traverse easily without any cost. The reads on the blockchain are free but writes cost (GAS)[2]

Origin of Blockchain

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize rate with which blocks are added to the chain.[6] The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network

Ethereum

Ethereum is a global, open-source platform for decentralized applications.

On Ethereum, you can use JS or solidity to write smart contracts [1] to interact with the blockchain. It's one of the finest blockchain platform available to make dapps.

Smart Contracts

It is an auto executing piece of code or contract which functions only when certain conditions are met. It lives in the middleware of every blockchain.

Ganache

It is an opensource local blockchain tool created for development and testing. It works exactly like a real blockchain and provides handy tools such as project imports, transaction display etc.

Solidity

It is a restricted ,object oriented ,high-level language based on JavaScript,C++ and python and is designed to target the Ethereum Virtual Machine (EVM). It is used to create smart contract which executes on the blockchain[10].

HTML

It was released in early 1993. It’s designed is so simplistic that it never got replaced by anything else.Hypertext Markup Language (HTML) is the standard markup language for documents designed to be displayed in a web browser. You can make plan web pages with just using html and it will work. But you need other things like CSS and JS to make it interactive and beautiful.

JavaScript

It is a light weight client scripting language to make webpage dynamic. Its syntax is similar to its parent java but provides few inbuilt functions which are related to web-based interaction.

Since JavaScript is interpreted it doesn’t require time in compiling hence fast.

Bootstrap

It is a light weight CSS framework with grid system that allows the modification of the HTML elements on the fly with no cost to the service. It also a client-side framework. Its idealology was built once run everywhere.Currently Bootstrap 5 is released its quite faster than previous generation but there are no major changes in the flow of the framework.

CSS

CSS stands for cascading styled sheet. It adds styling to the plain html elements so that they look more pleasing to the eye. With it we are able to create sites with eye catching animations and effects. There are various css frameworks available like Tailwind CSS and Bulma and bootstrap. Every framework got their own functions . The easiest if bootstrap . It automatically makes the site responsive for various screen sizes.

Problem Statement

All the existing voting systems lack security, transparency and efficiency.[13] When we vote for a candidate we don’t know if our vote is casted to him or not. Also, humans have a tendency to do bad things under pressure of money, power and greed. We need a fool proof system which provides us a guarantee and cost less than the previous one as the Evms needs maintenance and regular security check-up and transportation and storage cost .[9]

The cost of transferring evms back and forth from the storage location to polling centers is also significant. And who knows what happens when the transfer of the evms begins after the polling.

Motivation

The reason for learning blockchain was to increase my knowledge about it. How they function, why blockchain is the new standard of managing transactions. Since everything in today's modern world is a transaction. We innovated our way from file system to database then SQL databases to NOSQL databases for enhanced upscaling. But we didn't do much in regards of improving the security of them. We can you blockchain just like database. Unlike most of the database which are centralized it works of the opposite technology.

I was amazed by learning the fact about decentralization and how it provides transparency.

Objective

This project will solve the problem of security and fix any fraudulent activity. Blockchain is paving the way for a direct democracy. The rules of political parties and the elections needs to be changed so that they can be transparent and support blockchain environment.

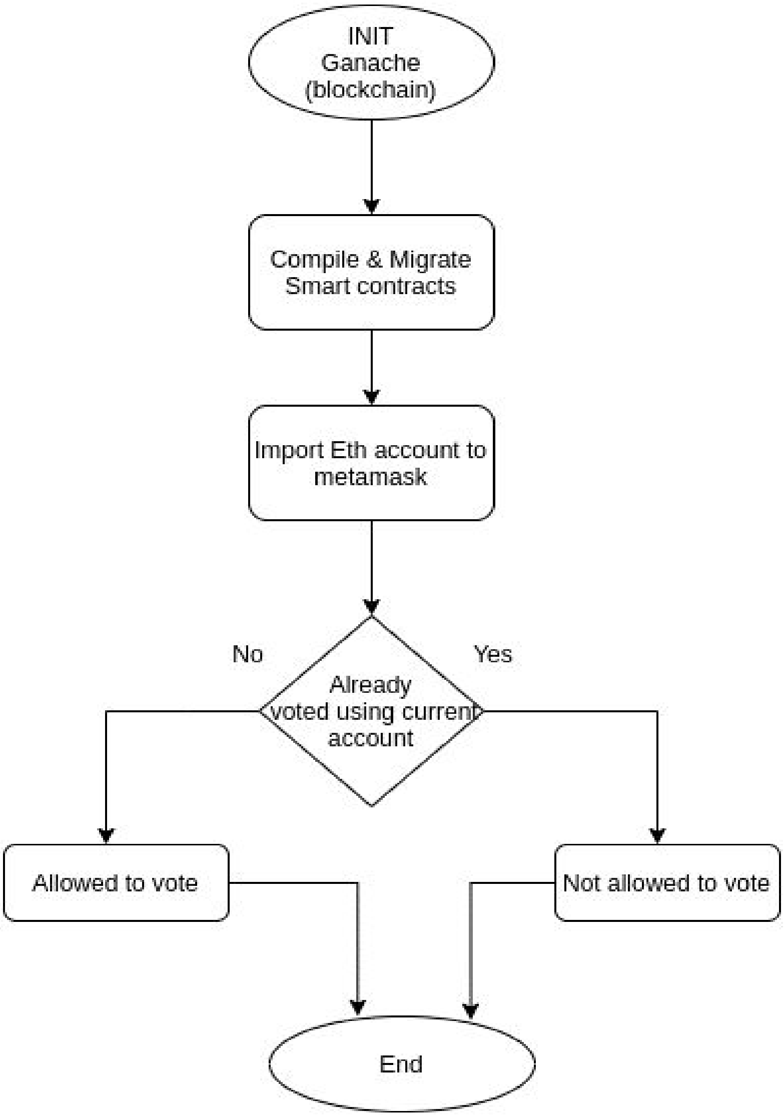
We can show super-fast results after elections are done since all the blocks are connected, we can run query and visualize the data and find the winning candidate within minutes or even seconds. This app will gain confidence as everything is transparent and immutable after being created (vote casted). This app will cost less than the traditional EVM [4] and the cost of the people for security and transport. It is the true digital version of the voting process.

SDLC Model

This I have used AD HOC (build and fix) model [6], since I was alone in the project I have all the control over the project.At first I was using IBM’s blockchain platform(Hyperledger)[7] but it was very restrictive , it was difficult to find the solutions of the bugs ,then I made my switch to Ethereum Virtual Machine. I made several revisions of the project and used git for version controlling. I knew what I wanted and got it right. Except the Aadhaar api[8] connectivity.

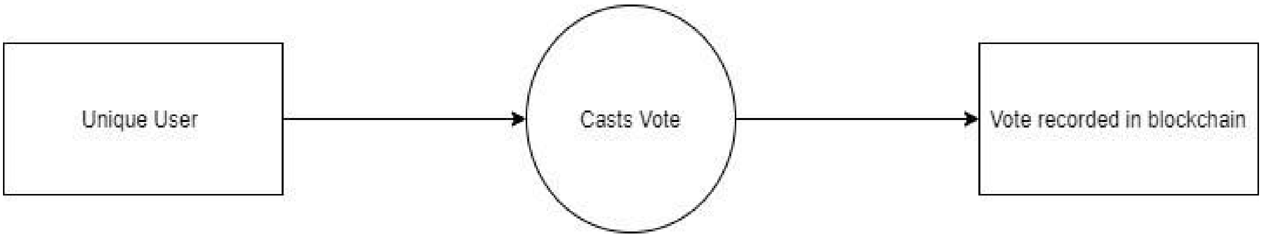
Flow Chart

This flowchart shows the sequential flow of the dapp. From initial state to the final state.

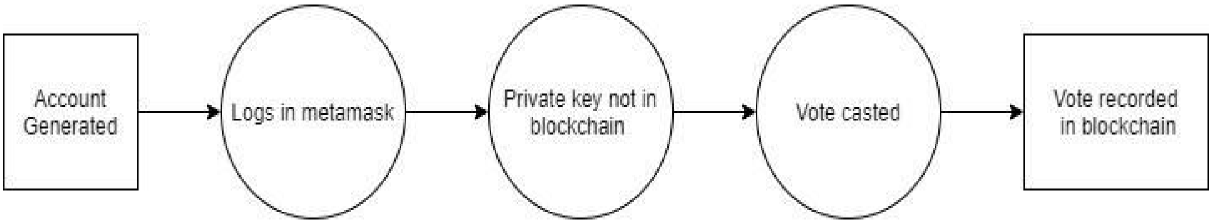

INIT
Ganache
(blockchain)
Compile & Migrate Smart contracts
Import Eth account to metamask
No
Yes
Already voted using current account
Allowed to vote
Not allowed to vote
End

Data Flow Diagram

Level 0



Level 1



Hardware and Software Requirements

HARDWARE REQUIREMENT:

1. RAM: 2GB or more

2. Processor: 1.2 GHz or Higher Processor

3. Storage: 100GB or more live free space on server

4. Screen resolution: minimum 1024x768

5. Sound Peripheral: headphones, speakers

6. Internet: 512kbps min

SOFTWARE REQUIREMENT:

1. Web Browser: Chrome, Firefox, Safari

2. MetaMask: Extension to convert browser into blockchain browser

3. Truffle.js: A opensource blockchain framework for Ethereum based network

4. Web3.js: It act as a interface between a eth node and browser over http.

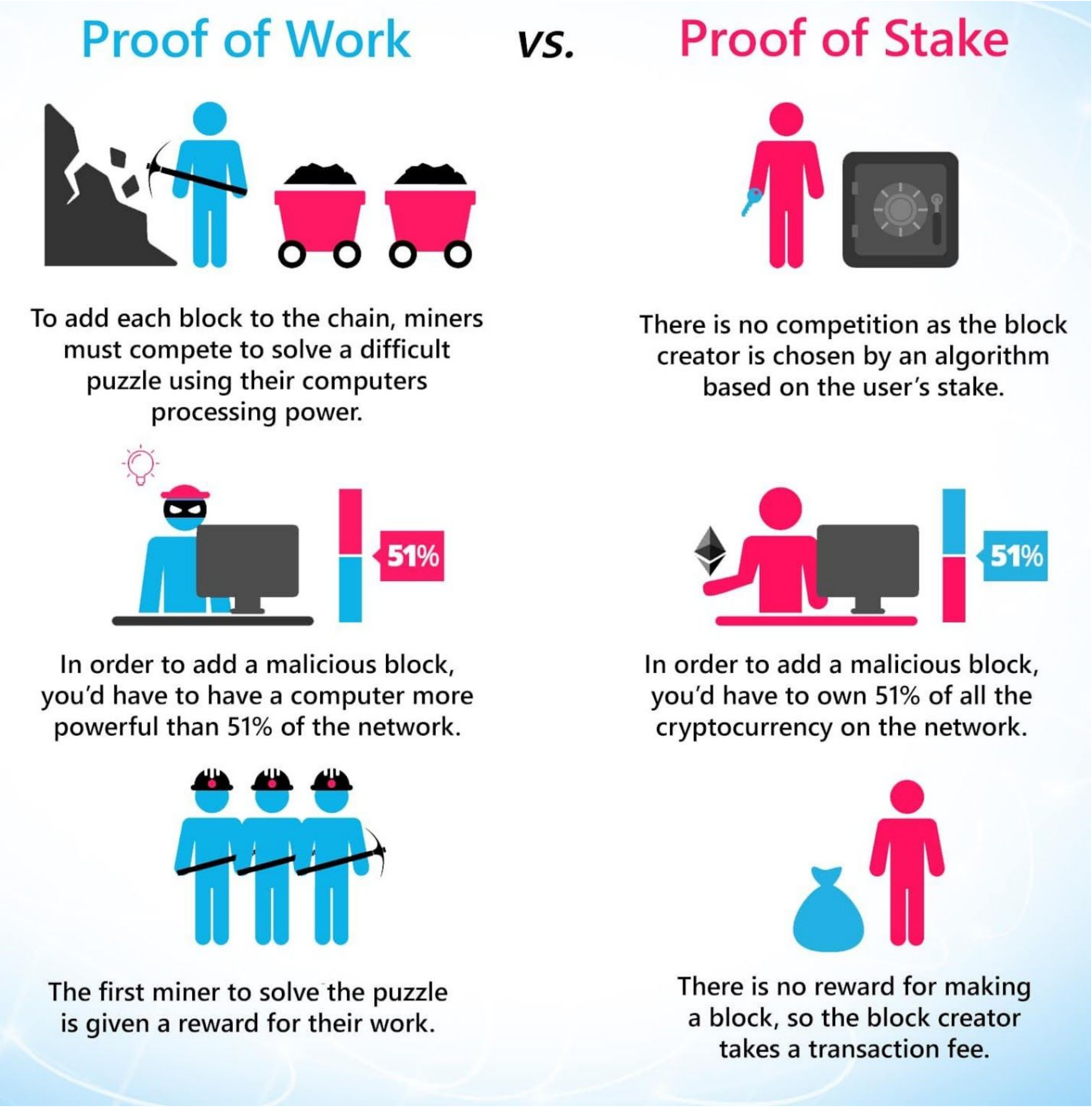
5. Node: It is a opensource runtime environment which allows a js code to be executed outside the web browser.

6. Ganache: One click blockchain (Local) tool which also generates accounts with fake Ether

7. Code Editor: Vs code, Sublime, Atom etc.

8. jQuery: A fast, small and feature rich JS library.

Proof of work vs Proof of stake



Proof of Work vs. Proof of Stake

To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.

In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.

The first miner to solve the puzzle is given a reward for their work.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

There is no reward for making a block, so the block creator takes a transaction fee.

[14].

Simulation

I’ve created smart contract with solidity called Election.sol . Used truffle.js to compile and migrate it to the local blockchain created using ganache tool. The output of contracts compilation is a JSON file. Which is used by truffle.js to interact with the blockchain. Ganache by default generates 10 accounts with fake ether. To interact with the blockchain.

The genesis block is created with the candidates (4) with 0 votes initially. Only one person/account is allowed to vote once. If a vote is casted using that account then the logged in can’t see the vote button and vote again.
Web3 is used to get the accounts from blockchain. Only blockchain’s connected accounts are allowed to vote.

For testing mocha framework is used. Total 5 test cases.

1. For 4 candidates.
2. For correct values(name and 0 votes)
3. For allowing a account to vote
4. Throwing exception for invalid candidate(>4)
5. Throwing exception for double voting.

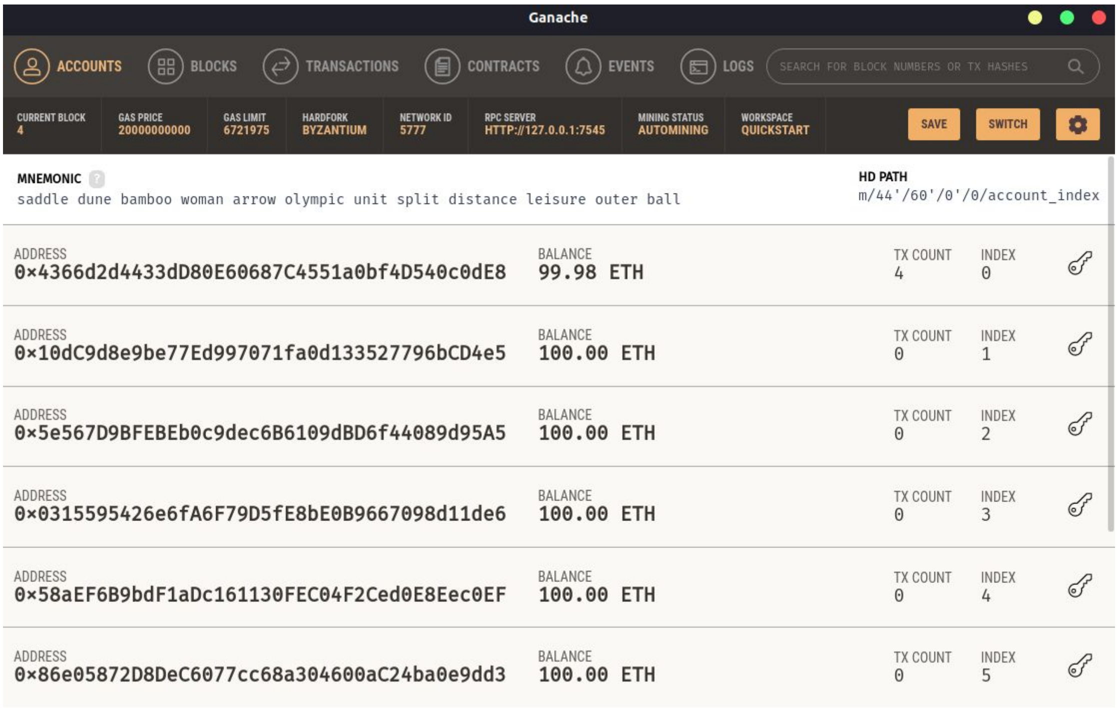
The App.js contains a object with 5 vars and 7 functions along.

There is a pie.js file which generates a pie chart on the basis of current vote casted on the blockchain from genesis to latest block.

Currently the dapp is build using JavaScript, html5, bootstrap. I will migrate it to react or vue before final submission. It will not require any refresh then only the components that are changed will automatically render themselves . Currently the dapp requires refresh automatically after the vote haven been casted.

Screenshots

1. Initializing Ganache (Local blockchain tool) will generate accounts specified which in this case was 10.



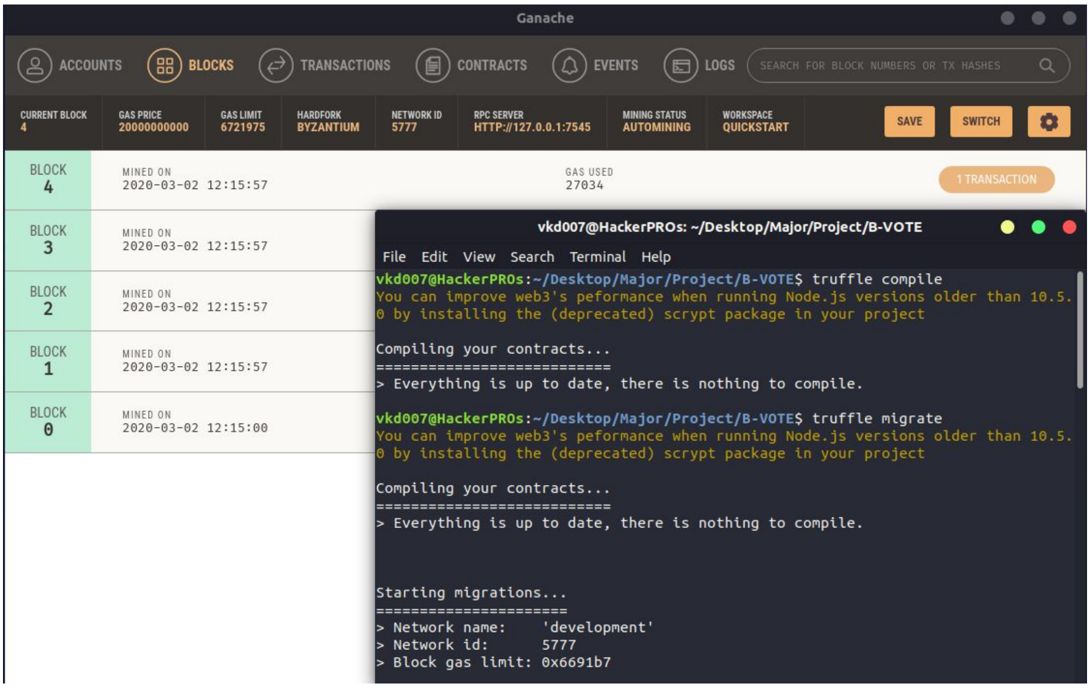
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	BYZANTIUM	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
saddle dune bamboo woman arrow olympic unit split distance leisure outer ball

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

ADDRESS	BALANCE	TX COUNT	INDEX
0×4366d2d4433dD80E60687C4551a0bf4D540c0dE8	99.98 ETH	4	0
0×10dC9d8e9be77Ed997071fa0d133527796bCD4e5	100.00 ETH	0	1
0×5e567D9BFEBEb0c9dec6B6109dBD6f44089d95A5	100.00 ETH	0	2
0×0315595426e6fA6F79D5fE8bE0B9667098d11de6	100.00 ETH	0	3
0×58aEF6B9bdF1aDc161130FEC04F2Ced0E8Eec0EF	100.00 ETH	0	4
0×86e05872D8DeC6077cc68a304600aC24ba0e9dd3	100.00 ETH	0	5

2. Compiling and deploying smart contracts. The contract will be called and blockchain will come into existence with a genesis block.

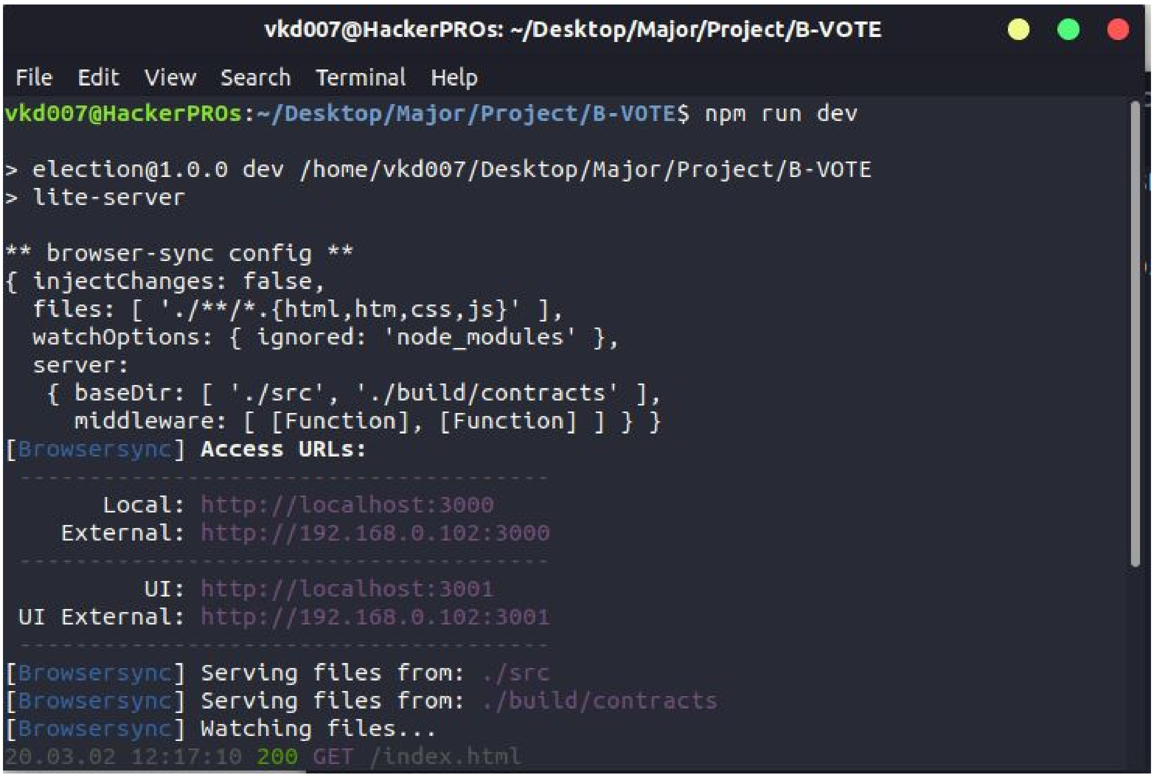


CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	BYZANTIUM	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

BLOCK	MINED ON	GAS USED
4	2020-03-02 12:15:57	27034
3	2020-03-02 12:15:57	
2	2020-03-02 12:15:57	
1	2020-03-02 12:15:57	
0	2020-03-02 12:15:00	

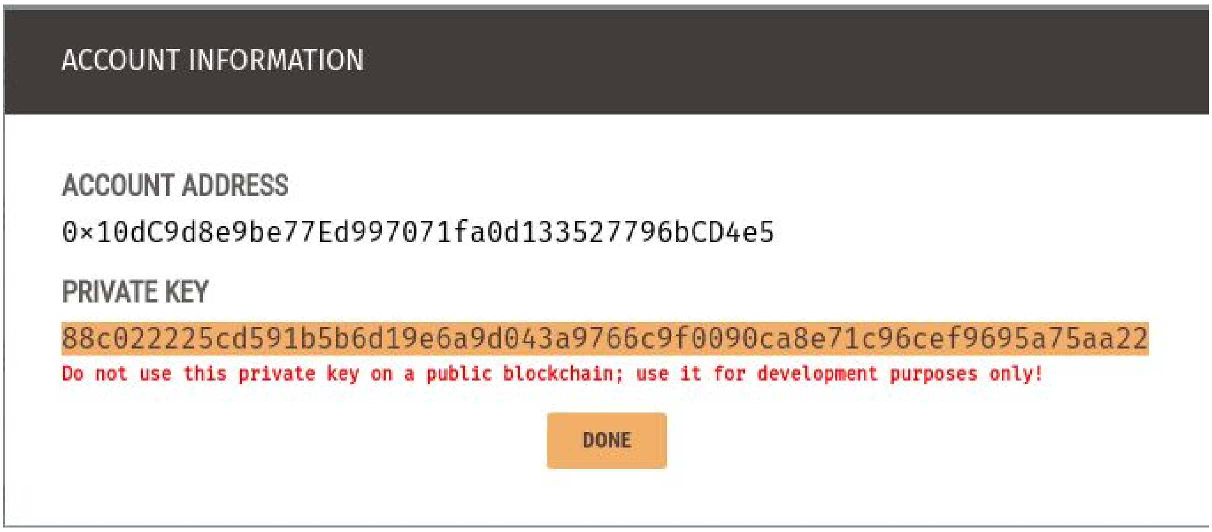
```
vkd007@HackerPROs:~/Desktop/Major/Project/B-VOTE$ truffle compile
You can improve web3's peformance when running Node.js versions older than 10.5.
0 by installing the (deprecated) scrypt package in your project

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.

vkd007@HackerPROs:~/Desktop/Major/Project/B-VOTE$ truffle migrate
You can improve web3's peformance when running Node.js versions older than 10.5.
0 by installing the (deprecated) scrypt package in your project

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 0x6691b7
```

3. Hosting the dapp on the localhost using lite-server along with browser sync module.


vkd007@HackerPROs: ~/Desktop/Major/Project/B-VOTE
File Edit View Search Terminal Help

```
vkd007@HackerPROs:~/Desktop/Major/Project/B-VOTE$ npm run dev

> election@1.0.0 dev /home/vkd007/Desktop/Major/Project/B-VOTE
> lite-server

** browser-sync config **
{ injectChanges: false,
  files: [ './**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server:
   { baseDir: [ './src', './build/contracts' ],
     middleware: [ [Function], [Function] ] } }
[Browsersync] Access URLs:
 --------------------------------------
       Local: http://localhost:3000
    External: http://192.168.0.102:3000
 --------------------------------------
          UI: http://localhost:3001
 UI External: http://192.168.0.102:3001
 --------------------------------------
[Browsersync] Serving files from: ./src
[Browsersync] Serving files from: ./build/contracts
[Browsersync] Watching files...
20.03.02 12:17:10 200 GET /index.html
```

4. Copying the private key of one of the accounts from ganache.


ACCOUNT INFORMATION

ACCOUNT ADDRESS

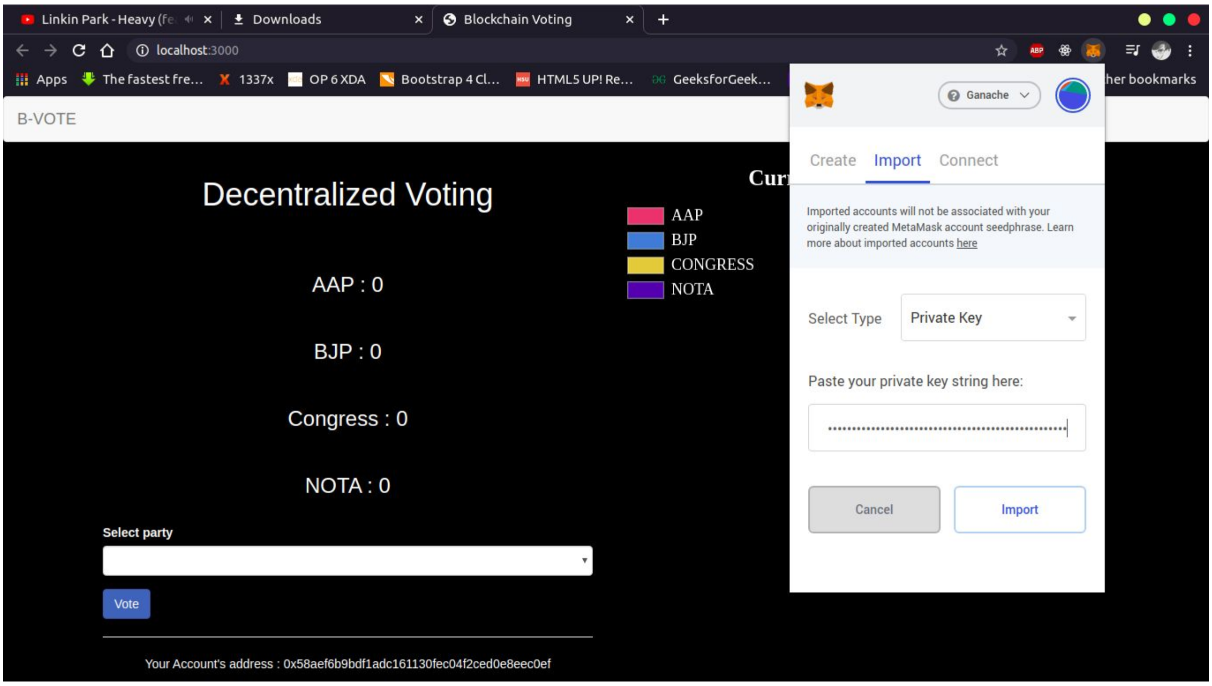
0x10dC9d8e9be77Ed997071fa0d133527796bCD4e5

PRIVATE KEY

88c022225cd591b5b6d19e6a9d043a9766c9f0090ca8e71c96cef9695a75aa22

Do not use this private key on a public blockchain; use it for development purposes only!

5. Inserting the private key into the metamask extension which connects the blockchain to the browser.



B-VOTE

Decentralized Voting

AAP : 0

BJP : 0

Congress : 0

NOTA : 0

Cur

🟥 AAP
🟦 BJP
🟨 CONGRESS
🟪 NOTA

Imported accounts will not be associated with your originally created MetaMask account seedphrase. Learn more about imported accounts here

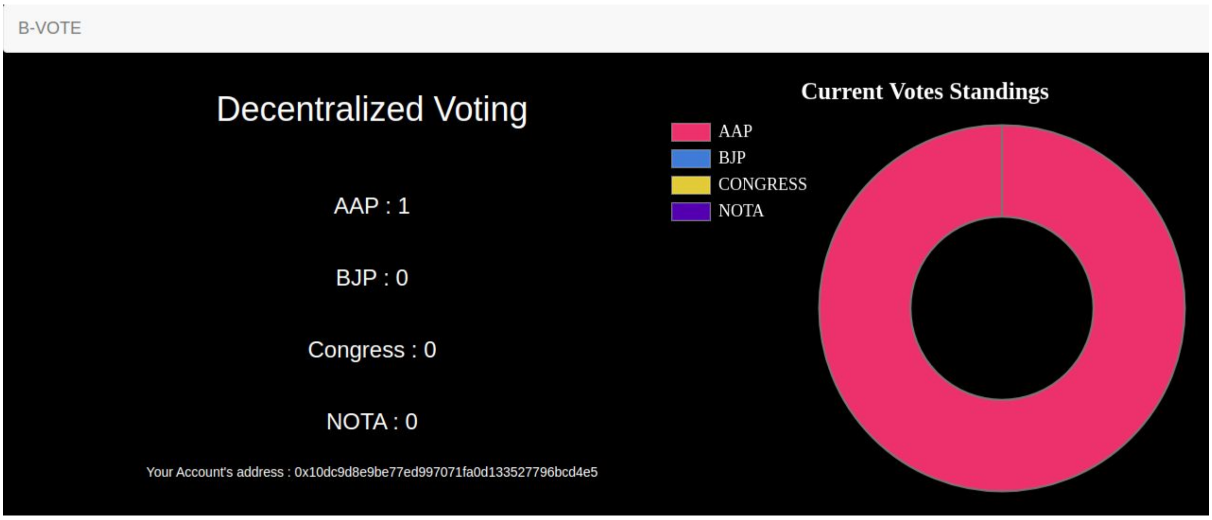
Select Type: Private Key

Paste your private key string here:

Select party

Your Account's address : 0x58aef6b9bdf1adc161130fec04f2ced0e8eec0ef

6. After voting using the account imported the vote button hides and the pie chart is displayed with the current standings.



B-VOTE

Decentralized Voting

AAP : 1

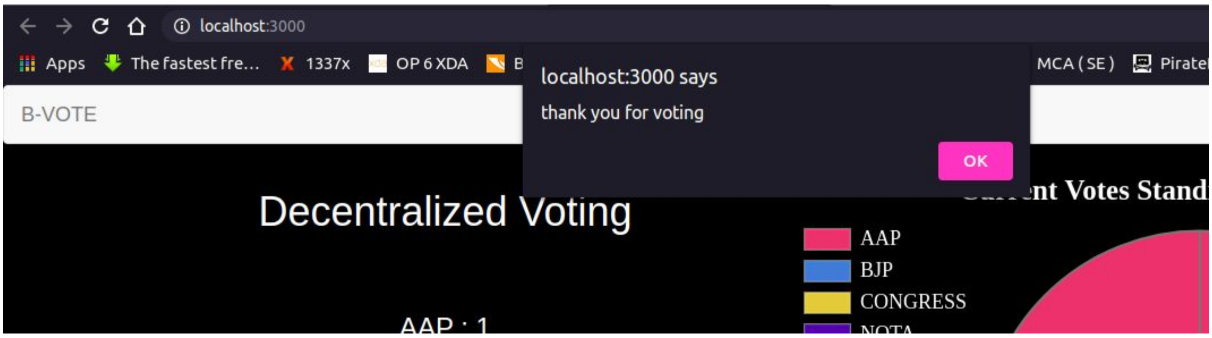
BJP : 0

Congress : 0

NOTA : 0

Your Account's address : 0x10dc9d8e9be77ed997071fa0d133527796bcd4e5

7. This alert pops up after you successfully vote for a party. If there's a popup that means the vote has been cast successfully.



B-VOTE

localhost:3000 says

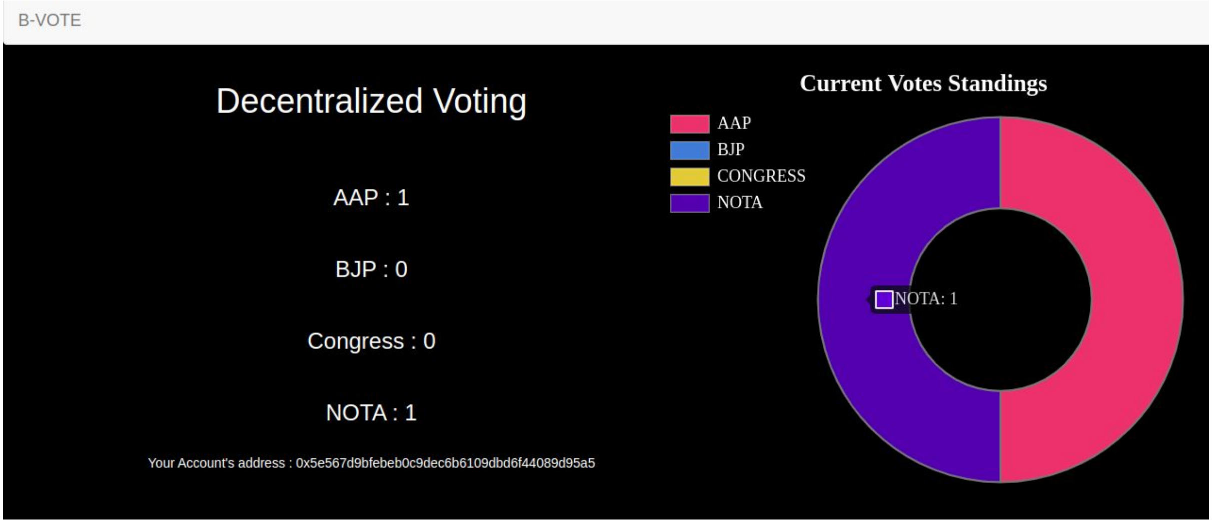
thank you for voting

Decentralized Voting

...ent Votes Stand...

AAP : 1

8. After voting once again the vote button hides itself and pie chart updates on refresh. The pie chart shows the current votes which the respective parties got.



B-VOTE

Decentralized Voting

Current Votes Standings

AAP : 1

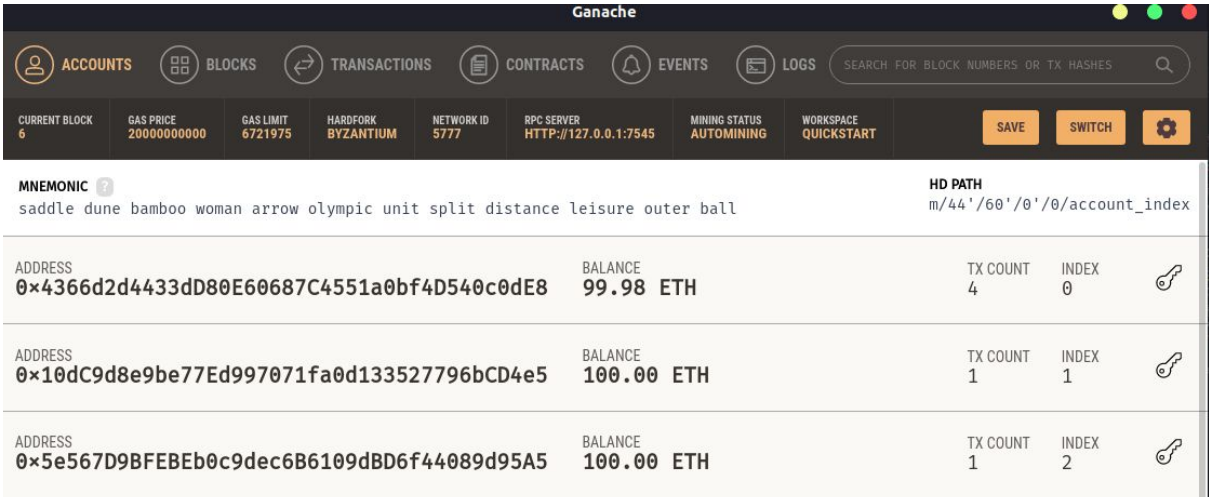
BJP : 0

Congress : 0

NOTA : 1

Your Account's address : 0x5e567d9bfebeb0c9dec6b6109dbd6f44089d95a5

9. The initial blockchain without a transaction from the dapp was 4 blocks but after voting twice the blocksize increased with 2 more blocks.



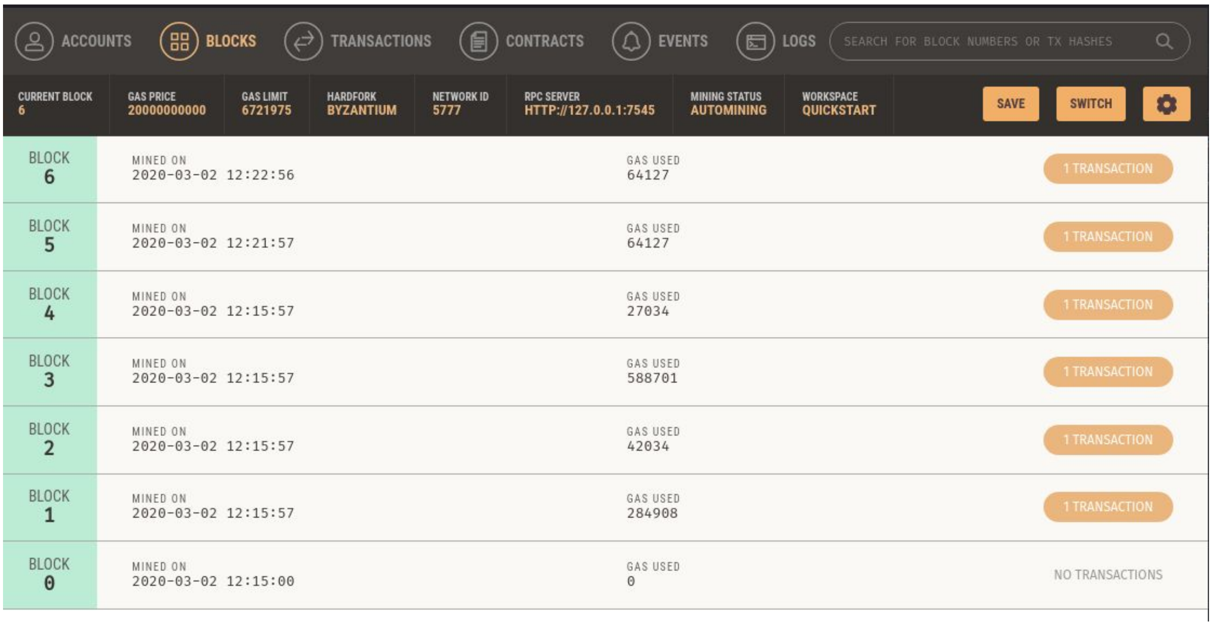
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
6	20000000000	6721975	BYZANTIUM	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
saddle dune bamboo woman arrow olympic unit split distance leisure outer ball

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

ADDRESS	BALANCE	TX COUNT	INDEX
0x4366d2d4433dD80E60687C4551a0bf4D540c0dE8	99.98 ETH	4	0
0x10dC9d8e9be77Ed997071fa0d133527796bCD4e5	100.00 ETH	1	1
0x5e567D9BFEBEb0c9dec6B6109dBD6f44089d95A5	100.00 ETH	1	2

10. You can see the blocks in ganache tool the date and time of the new block creation.



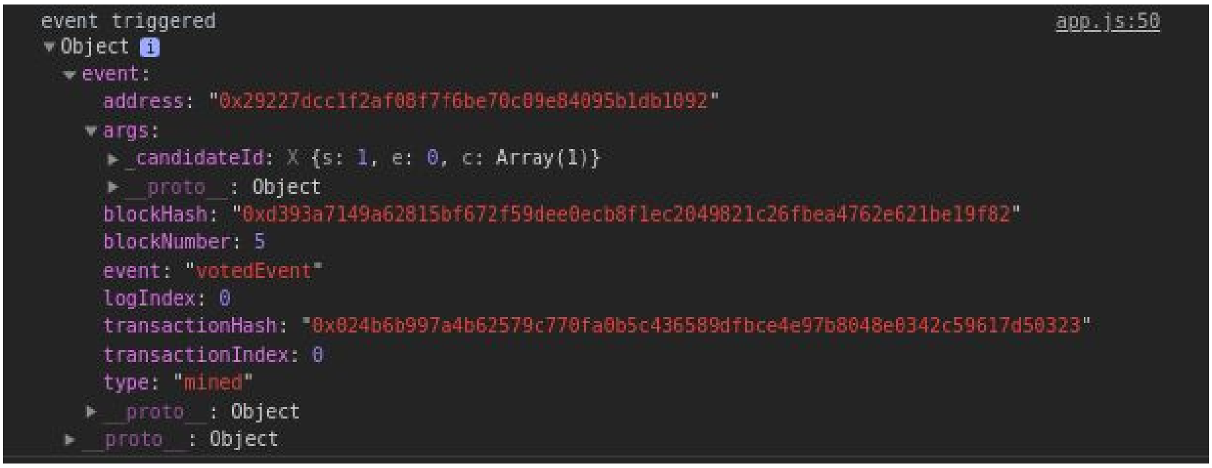
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
6	20000000000	6721975	BYZANTIUM	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

BLOCK	MINED ON	GAS USED	
6	2020-03-02 12:22:56	64127	1 TRANSACTION
5	2020-03-02 12:21:57	64127	1 TRANSACTION
4	2020-03-02 12:15:57	27034	1 TRANSACTION
3	2020-03-02 12:15:57	588701	1 TRANSACTION
2	2020-03-02 12:15:57	42034	1 TRANSACTION
1	2020-03-02 12:15:57	284908	1 TRANSACTION
0	2020-03-02 12:15:00	0	NO TRANSACTIONS

Analysis of Transactions

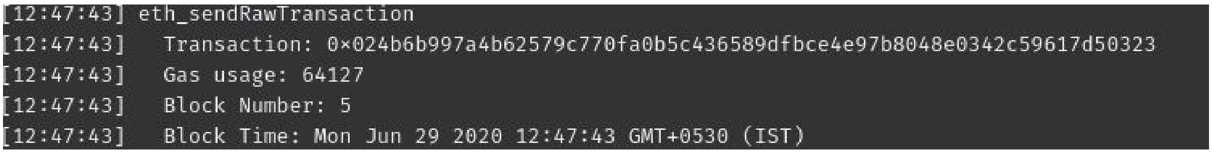
Whenever a person click on the vote button he is able to vote and if the transaction is successful then block hash and transaction hash are generated.

This Screenshot is from the browser. object stores all the information about the transaction.It also shows the even which happened (votedEvent) which is a function in the codebase.



```
event triggered                                                                app.js:50
▾Object ℹ
  ▾event:
     address: "0x29227dcc1f2af08f7f6be70c09e84095b1db1092"
    ▾args:
      ▸_candidateId: X {s: 1, e: 0, c: Array(1)}
      ▸__proto__: Object
     blockHash: "0xd393a7149a62815bf672f59dee0ecb8f1ec2049821c26fbea4762e621be19f82"
     blockNumber: 5
     event: "votedEvent"
     logIndex: 0
     transactionHash: "0x024b6b997a4b62579c770fa0b5c436589dfbce4e97b8048e0342c59617d50323"
     transactionIndex: 0
     type: "mined"
    ▸__proto__: Object
  ▸__proto__: Object
```

This Screenshot is from the Ganache Local blockchain tool. Here we can only see the amount of gas used and the no of block and transaction hash.



```
[12:47:43] eth_sendRawTransaction
[12:47:43]   Transaction: 0×024b6b997a4b62579c770fa0b5c436589dfbce4e97b8048e0342c59617d50323
[12:47:43]   Gas usage: 64127
[12:47:43]   Block Number: 5
[12:47:43]   Block Time: Mon Jun 29 2020 12:47:43 GMT+0530 (IST)
```

Limitations

Blockchains are immutable. Chances of human error in data is huge so when a person makes a mistake it will be stored forever. At the current state of blockchain the development is quite difficult as it is still a growing industry. There are few open source libraries but they lack in functions. For which you would have to include another library. Also blockchain requires a block network which is easily available for localhost via Ganache or Ganache CLI but to publish it on the web its quite difficult.

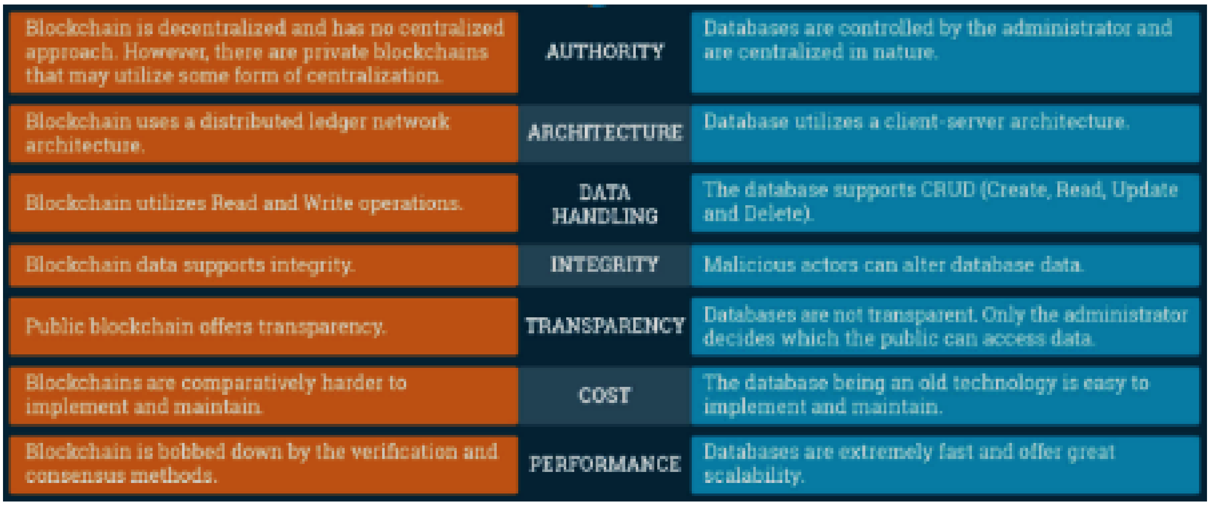
Since blockchains are transparent its data is visible to all users. So if your Access is the biggest thing in a system to play with functionality and that here has limited the game altogether!

Also, blockchain systems require more resources than the traditional system. Since the ledgers of all the nodes are to be updated after every transitions.

Comparison to Traditional System

Both of the systems have their caveats and advantages but the blockchain system beats the traditional one(DB) in terms of security and transparency. Since after voting for a candidate in a traditional system you aren't 100% sure that he/she received it but in case of blockchain based voting app it's visible and non editable so once a vote is granted it can't be changed.

Every other node can see the ledger or the (information) of other block that is why it is transparent. Consensus methods are used to verify the transactions like POW and POS.



Blockchain is decentralized and has no centralized approach. However, there are private blockchains that may utilize some form of centralization.	AUTHORITY	Databases are controlled by the administrator and are centralized in nature.
Blockchain uses a distributed ledger network architecture.	ARCHITECTURE	Database utilizes a client-server architecture.
Blockchain utilizes Read and Write operations.	DATA HANDLING	The database supports CRUD (Create, Read, Update and Delete).
Blockchain data supports integrity.	INTEGRITY	Malicious actors can alter database data.
Public blockchain offers transparency.	TRANSPARENCY	Databases are not transparent. Only the administrator decides which the public can access data.
Blockchains are comparatively harder to implement and maintain.	COST	The database being an old technology is easy to implement and maintain.
Blockchain is bobbed down by the verification and consensus methods.	PERFORMANCE	Databases are extremely fast and offer great scalability.

[15]

Conclusion

The idea of adapting blockchain voting system to make public elections cheaper, faster and secure is compelling in this advance era. Its not only better and efficient than the EVMS but also more reliable and secure.

It is not possible for any account to vote without any ether in that account and are not mined on that blockchain. So, it is safe to say that no external entity can vote. To make changes to the blockchain the external entity must hold all the nodes in physical possession and do 51% attack which is impossible if we have 100+ nodes.

So with Aadhar Api the project will be fully ready for deployment and can be tested so that it can be used for future elections.

Future Scope

The current scenario is the blockchain transactions require mining (which is costly). If a user wants to do a transaction it requires to have some coins or Ethereum[1] in my case. Without it it's not possible to vote. And there are no blockchain platform available for mobile devices. So, REST api[11] can be made so that it can be ported to mobile apps and users can cast vote from mobile. Also, a foolproof way to validate user is required. I was hoping to integrate Aadhaar api in the project but the govt still haven't replied me. So, the project just needs Adhaar api or Voter Id api to create user and provide them with some coins to cast the vote.

Also the Web App should be deployed on the cloud as the no of users increases the system will require more CPU and memory. AWS or GCP [12] are the best possible options present ,as both supports auto scaling and different types of cpu and os .Currently the system requires unix based os to run but it can also use windows platform with few minor tweaks.

References

1. https://ethereum.org/
2. Blockchain: Blueprint for a new economy (February 2015) ISBN : 978-1-491-92049-7
3. https://www.youtube.com/watch?v=32F3X1E121A
4. https://eci.gov.in/evm/
5. https://www.udacity.com/course/blockchain-developer-nanodegree–nd1309
6. https://www.academia.edu/11766757/Comparative_Study_of_Various_SDLC_Models_on_Different_Parameters
7. Performance Characterization of Hyperledger Fabric (CVCBT 2018)
8. https://www.uidai.gov.in/914-developer-section.html
9. https://www.quora.com/How-much-approximately-does-an-electronic-voting-machine-EVM-cost-Do-we-import-them-or-do-we-make-them-in-India
10. https://solidity.readthedocs.io/en/v0.6.7/
11. Analysis of REST API Implementation (ISSN : 2456-3307)
12. Comparative Study of Cloud Services Offered by Amazon, Microsoft & Google (2456-6470)
13. Nicholas Weaver (2016). Secure the Vote Today. https://www.lawfareblog.com/secure-vote-today
14. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
15. https://101blockchains.com/blockchain-vs-database-the-difference