CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF VOTING SYSTEM

The most fundamental aspect of a democracy is the avail- ability for citizens to not only share ideas, opinions, and beliefs but to make their individual voices heard by deciding the collective future by vote. However, for the voting to proceed as intended, there needs to be a transparent and secure process where also the voters knowingly keep their privacy. The challenge is to find a solution that prevents unlawful manipulation of the collected data and achieve desired transparency in the security measures, taken to protect voter privacy and the collected results and therefore democracy itself. By using blockchain our proposed system has the features like security, privacy, and integrity. In blockchain every node or user is anonymous and every action performed is a transaction which is hashed and then stored into the network.

To test our protocol, we put it on Ethereum a blockchain platform that uses Solidity as a programming language to create smart contracts. Smart Contracts are backbone of Blockchain System. The usage of smart contracts ensures a safe means for performing voter verification, ensuring the correctness of voting results, making the counting system public, and protecting against fraudulent activities. Blockchain Technology eliminates the risk of single point of failure, which is usually seen in traditional approaches as discussed above, making our voting system tamperproof and trustworthy which not only provides integrity to voters or citizens, but also supports transparency among voters and candidates and it also strengthens the actual meaning of democracy and create a sense of belief among them and thus making the system more secured and reducing the cost for infrastructure management as well. Voting is a process which is defined as the right of people to choose their leaders. Voting is a important process that enables people to handpick their government leader.

The voting system should be democratic, independent, and unprejudiced. As a result, it must be a transparent and secure procedure that allows everyone to partake their standpoint freely. A lot of people in the world do not keep faith in the election system.

The Traditional voting is controlled and full of mediators. Fur- thermore, people are dealing with a variety of issues, such as booth capture, dummy voting and the problem of proper monitoring, a massive line of people in front of the polling booths, false voting, pre-vote casting, redundant vote, lack of awareness, polling booths are located a long distance away from the house, etc. The above problems can be solved using Blockchain technology which will provide a reliable system, where one can trust the system with integrity. Blockchain is a decentralized network in which the node members exchange data, but each user maintains the identical data replication. Blockchain technology provides characteristics such as pri- vacy, and data accuracy, etc.

1.2 AIM OF THE STUDY

Current voting systems like ballot box voting or electronic voting suffer from various security threats such as DDoS attacks, polling booth capturing, vote alteration and manipulation, malware attacks, etc, and also require huge amounts of paperwork, human resources, and time. This creates a sense of distrust among existing systems.
Some of the disadvantages are:

- Long Queues during elections.
- Security Breaches like data leaks, vote tampering.
- Lot of paperwork involved, hence less eco-friendly and time-consuming.
- Difficult for differently-abled voters to reach polling booth.
- Cost of expenditure on elections is high.

1.3 SIGNIFICANCE OF THE STUDY

Using blockchain, voting process can be made more secure, transparent, immutable, and reliable.
Suppose you are an eligible voter who goes to polling booth and cast vote using EVM (Electronic Voting Machine). But since it's a circuitry after all and if someone tampers with microchip, you may never know that did your vote reach to person for whom you voted. Since there's no tracing back of your vote. But, if you use blockchain- it stores everything as a transaction that will be explained soon below; and hence gives you a receipt of your vote (in a form of a transaction ID) and you can use it to ensure that your vote has been counted securely.
Now suppose a digital voting system (website/app) has been launched to digitize process and all confidential data is stored on a single admin server/machine, if someone tries to hack it or snoop over it, he/she can change candidate's vote count- from 2 to 22! You may never know that hacker installs malware or performs clickjacking attacks to steal or negate your vote or simply attacks central server.

To avoid this, if system is integrated with blockchain- a special property called immutability protects system. Consider SQL, PHP, or any other traditional database systems. You can insert, update, or delete votes. But in a blockchain you can just **insert data** but cannot update or delete. Hence when you insert something, it stays there forever and no one can manipulate it- Thus name immutable ledger.
But building a blockchain system is not enough. It should be decentralized that is if one server goes down or something happens on a particular node, other nodes can function normally and do not have to wait for victim node's recovery.

1.4 LIMITATION OF THE STUDY

One of the problems with e-voting is that it is almost impossible to satisfy all the requirements. Understand e-voting here as any voting system maintained over some form of hardware or software. We have several amazing and ingenious technologies to apply in these systems, but even so, they almost always require a trade-off.

1.5 PROBLEM STATEMENT

- In the current system, voting is done by using EVM(Electronic Voting Machine).
- This system can be replaced by the online voting(E-voting) system which will limit the voting frauds.
- Expanding e-voting into Blockchain technology could be the solution to alleviate the present concerns in e-voting.
- With this view in mind we are going to develop Online Voting system using Blockchain.
- This e-voting system has the potential to make the voting process easier and more accessible for electors.

1.6 METHODOLOGY

1.7 OVERVIEW OF THE STUDY

The thesis include the following chapters to achieve the Decentralized Voting System design.

Chapter 1: This is an introduction to the topic of the thesis. The summary of the study is outlined, which describes the purposes, significance, limitations, problem statements, methodology.

Chapter 2: Reviewing the use of techniques of blockchain. The discussion provide some relevant research works presented to solve the voting issues using blockchain technology.

Chapter 3: Briefly indicates summary about blockchain technology.

Chapter 4: Explains the basics of the methodology that contains designing a system for decentralized voting system. It explains about the proposed system, preliminary requirements and working.

Chapter 5: Represent the experimental result analysis .

CHAPTER 2

LITERATURE REVIEW

E-voting system was a great advancement over traditional pen and paper approach and became very popular in many countries. Several countries introduced e-voting system in their election process. Although it provided a number of advantages like increased voter turnout, auditability, low cost, convenient and accessible elections, etc. but there were several important challenges and issues associated with it.

Abdelwehab et al. in their study discussed a number of challenges in e-voting system including legal challenges, social and cultural challenges, technical challenges, attacks, etc.

Diego F. Aranha et al. in their work identified an experiment to test the validity of election results and to enhance transparency and voter participation within electronic elections. This proposal was based upon two aspects that is distributed collection of pole tape, made by mobile devices by voters and crowdsourcing election data verification by electoral authority.

Kristian Gjosteen and Anders Smedstuen believed that if voters make use of voting protocol correctly then there will be no chance of attack on results of elections and they give a statistical method to improve the security of e-voting.

Budurudhi et al. explores how to properly develop voting machine interfaces to promote the role of electors and electoral administrators and then use such interfaces for complex elections. The problem of relying on a remote voting device is said to be firmly linked to the interface provided which in turn influences votes as verification of voting is an important issue. Much of the work in remote– electronic voting involves cryptography voting protocols design and verification to safeguard desired property.

Neumann et al.states that in order to make specific recommendations on the type of voting system that is best suited to that particular context, they introduced a model for the comparison of voting schemes in any given electoral setting and the model was applied to the specific context of Estonian internet voting. As there were various problems with electronic voting especially related to physical security, people began to look for solutions to the problems that's when blockchain came into the field of e-voting, initially blockchain was used for bitcoin.

Ahmed Ben Ayed in his work discusses how to take the advantages of blockchain technology in the process of e-voting to make it safe, secure, anonymous, etc.

Jen-Ho Hsiao et al. in their work make use of smart contracts in decentralized blockchain technology for e-voting to engage all voters in evaluating and recording ballots. It increases the trust of electorate and decreases the misuse of election capital.

CHAPTER 3

BLOCKCHAIN TECHNOLOGY

3.1 BLOCKCHAIN TECHNOLOGY

Blockchain proved to be a substitute for the conventional approach by making system unalterable and transparent. Blockchain is an organized data structured that includes **blocks** where each block is connected to every other block through a chain. The first block is called as genesis block. Each new block will be stacked to form a stack called a blockchain. Each block consists of **data, hash and hash of previous block**. If any change is being made to the data available in a particular block, consequently the hash of the block also gets changed but the next block will have the same unchanged hash of the previous block which invalidates this block and all other succeeding blocks. This is to avoid tempering because making change in one block you will need to calculate hash for every other following block however hackers now a days can compute hundreds of thousands of hashes in a matter of seconds. In order to avoid this problem it makes use of proof-of-work concept that delays the pace of forming a new block. Moreover it make use of a distributed peer to peer network where no central entity is present. Whenever a new block gets created it is sent to all other nodes present on this network where each node makes sure that no tempering is done by verifying the block after which the new block is added to every other node's blockchain. Every node on the network agrees on whether the block is valid or not by creating a consensus which makes blockchain so secure, safe and reliable.

3.2 Smart contract:

A smart contract is a self-imposed contract that is embedded in a blockchain managed computer code. This code includes a set of rules governing the communication and decision on the contract between the parties, the contract will be enforced automatically once the already defined rules are met. Smart contract gives a framework for efficient control between two or more parties of tokenizes assets and access rights . Fig 1 ; shows the working principle of smart contract. Blockchain is just a database that cannot be altered, without smart contract, which expands and leverages blockchain

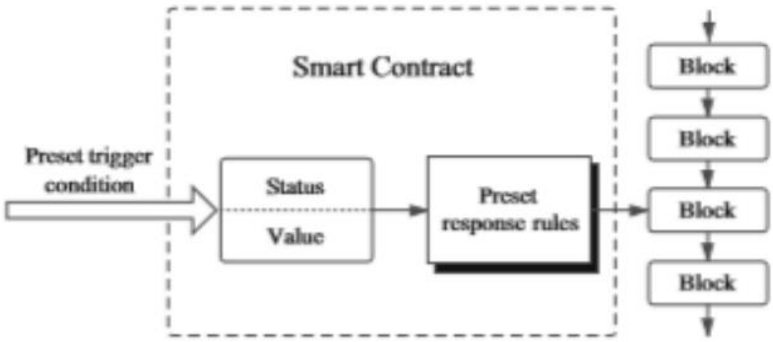

Fig: Smart Contract Working Principle

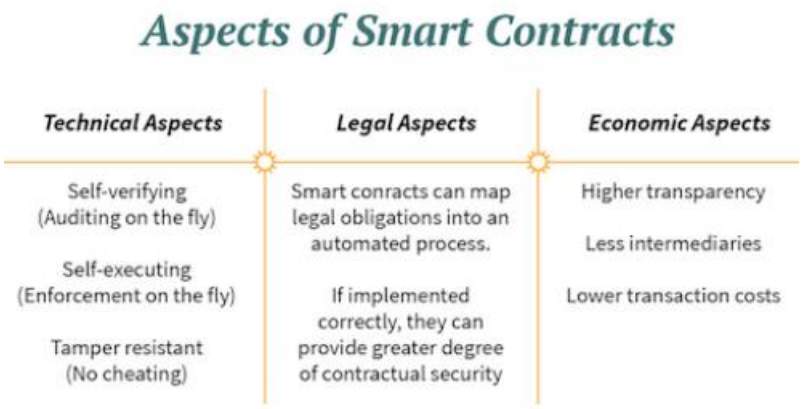

Fig 2: Various Aspects of Smart Contracts

Self-verification of the conditions in a smart contract is done by data interpretation. Each network node will guarantee the proper execution of a single contract, which relief the contract creators from tracking the execution of the contract. Smart contracts are self-executing, where the conditions of the agreement between different parties are written into the code. This means that legal obligations can be mapped using smart contracts into automated process. The execution of the contract can be automatically invoked by a trigger like expiration date. In this paper, we implement blockchain based e-voting system which overcome the problems encountered in e-voting and builds trust among voters for legitimate voting. Moreover, it will also be a helpful step towards the development of smart governance.

3.3 BLOCKCHAIN DATAFLOW

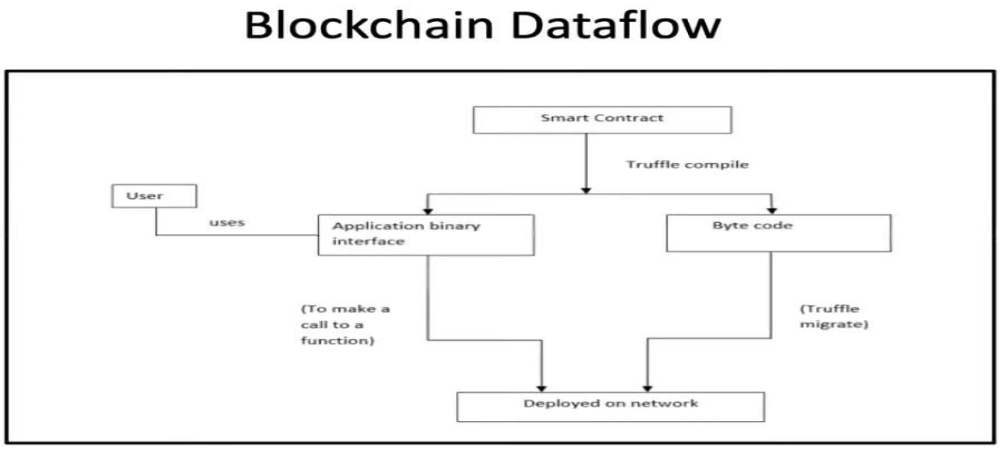

Fig 3: Blockchain Dataflow

CHAPTER 4

PROPOSED BLOCKCHAIN TECHNOLOGY FOR DECENTRALIZED VOTING SYSTEM

4.1 PROPOSED SYSTEM

The proposed system utilizes several tools namely ganache, truffle framework, Vs code, npm and meta mask. Truffle imports the smart contracts on the blockchain while as ganache operates the internal blockchain and it will be accessed by using meta mask. With some Ether i.e. Ethereum's cryptocurrency is required by a user for an account with wallet address. To write the transaction to blockchain, user needs to pay a certain transaction fee which is called as gas. Once votes are cast the process is completed by a number of nodes on the network called as miners. These miners compete with each other to complete the transaction. The miners who succeed in this transaction is awarded ether paid by users to vote. Instead of node we will be using ganache software for mining purpose.

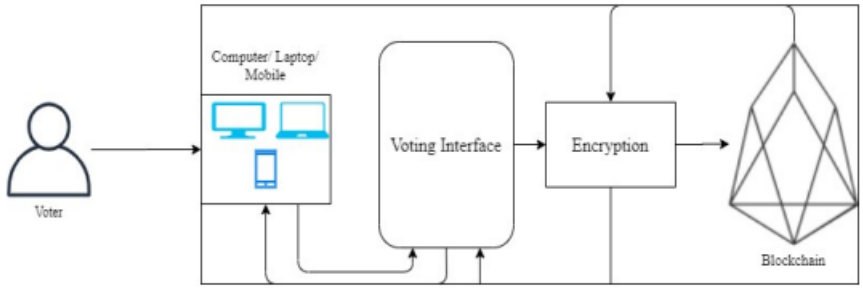

Fig 4: Proposed E-voting system based on Blockchain

4.2 PRELIMINARIES

Our proposed model can be implemented by using 64-bit hardware/ machine, windows 7 onwards, NMP dependencies, Truffle framework, Meta mask, solidity toolkit and Ganache.

1. Dependency NPM(Node Package Manager)

2. Truffle framework

3. Ganache

4. Meta mask

5. Coding language; solidity, HTML, JavaScript, CSS NPM (Node Package Manager): NPM is package manager that manages, installs, updates or uninstalls the node.js packages in an application. It is a command line based tool.

Truffle framework: Truffle is a powerful tool to work with ethereum smart contracts. It is used for compilation, deploying and linking of smart contracts, provides testing platform for automated contracts, manages networks and packages, etc.

Ganache: It was previously known as Testrpc and comes in both forms command line and UI. A virtual blockchain establishes ten standard Ethereum address with all and private key preloading them with simulated hundred ether each. With ganache there is no mining rather it automatically confirms every transaction. It is convenient for operating systems like windows, Linux and mac .

Meta mask: Meta mask is an open source, user friendly tool having a graphical user interface for doing transactions in ethereum. Ethereal D apps can run without having a complete ethereum node running your system browser. Meta mask is essentially a bridge between browser and blockchain ethereum.

Solidity: Solidity is a high-level language with JavaScript style syntax for contracts. It is a method for generating EVM machine level code and converts it into simple instructions. It has four value types namely: Boolean, Integer, Address and String but has same operators as that of JavaScript .

4.3 WORKING

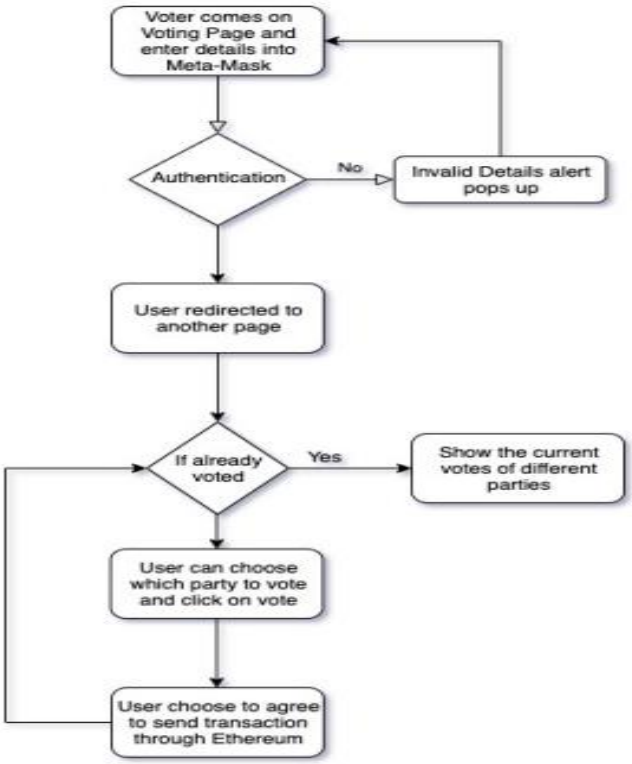

Fig 5: Flow model of voting system based on blockchain

The voter can log on to the voting website, then he has to log in with the Chrome Extension of Meta mask to connect with the local blockchain. Once the user is connected, the page is refreshed and the user can see the candidates and the current votes. Below that is the option to select the candidate to vote, the voter selects the candidate and click on vote, a meta mask pop-up comes up which tells the Ethereum transaction that has to be made, once the user clicks on Vote, the vote is given to the selected candidate provided that the voter hasn't voted before. If the user has already voted and attempts to vote again, a failed transaction will occur and vote will not be accounted.

A local blockchain is deployed using Ganache and meta mask is set up to connect with it. Truffle framework allows to migrate the smart contracts created on solidity to the local blockchain. When the user clicks to vote, meta mask allows to move Ether from one account to another. Every user is given a unique ID that is Ethereum Address and a private key and exact amount of Ether is distributed to all the voters' accounts. Once the user votes, the Ether is transferred from the voter's account to the Candidate's account, and all the transactions goes through the blocks, all the transactions will be visible to everyone once we launch the project. This will give voters complete transparency and they can cross-check their votes. Once the user has voted, the address will not contain the same amount of Ether, therefore if the user attempts to vote again, the transaction won't be completed and the vote will not be accounted. Mining is performed by all the other nodes but here, we have given Ganache the power to auto-mine on behalf of other nodes. The flowchart below explains the voter side of the process.

CHAPTER 5

RESULTS AND DISCUSSIONS

5.1 EXPERIMENTAL SETUP

5.1.1 Setting up:

The first thing that we need to do is run local blockchain by starting up Ganache.

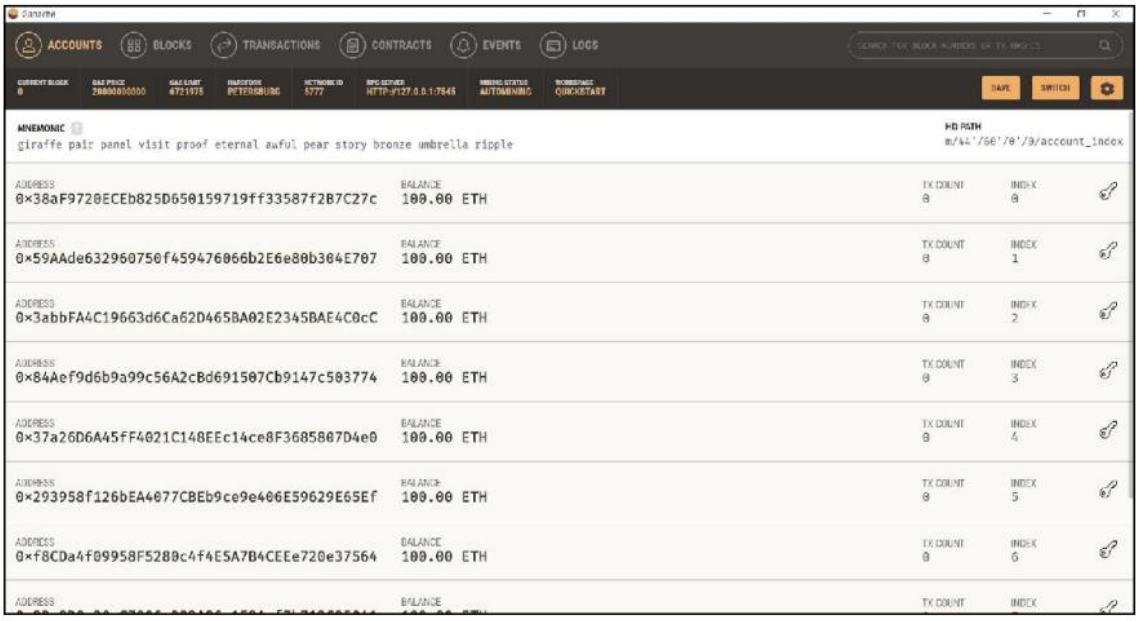

Fig 6: Setting up of Ganache

5.1.2 Login via meta mask

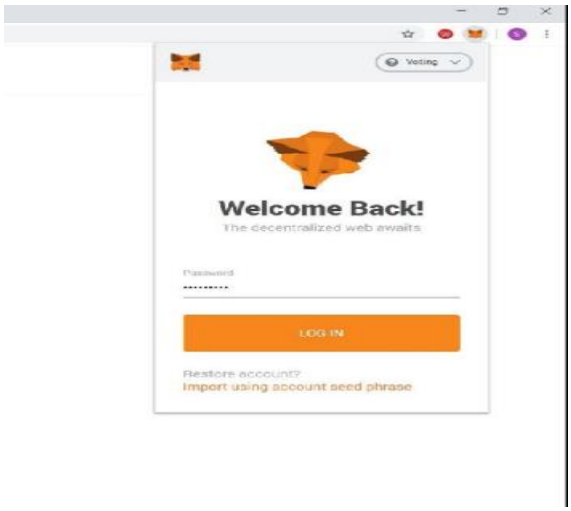

Fig 7: Constituency Logging In Via Meta mask.

5.1.3 Main Screen

After the user has logged in, main screen comes up with zero vote, the user cannot vote until they import their account by entering private key.

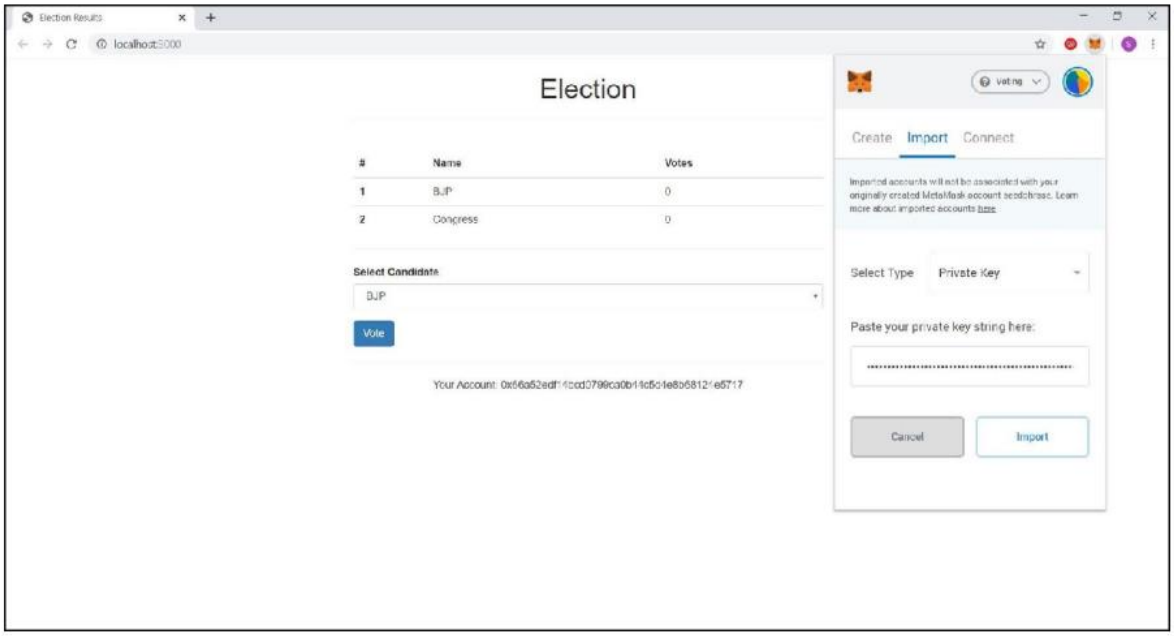

Fig 8: Main Screen

CHAPTER 6

CONCLUSION

The recent development in the area of voting system includes Blockchain technology, which not only proved to be time and cost efficient but is also safe and secure, hence is more reliable and precise than the earlier approaches. In this paper we have used blockchain based e- voting using smart contract which includes a set of rules governing the communication and decision on the contract between parties. Various tools like Ganache, Truffle framework, NPM and meta mask were used for implementation purpose. As blockchain technology is decentralized due to which tempering and alteration in such system is quite attainable. Our proposed system provides convenience to the voters by allowing them to connect to the system having easy-to-use user interface, through which they can cast their vote by importing their account and can easily review their vote. It creates a sense of trust among voters, that their vote is being computed and kept in a safe custody.

REFERENCES

[1] https://shermin.net/token-economy-book/

[2] Zhang, S., Wang, L. & Xiong, H. Int. J. Inf. Secur. (2019) Chain integrity: blockchain enabled large-scal e-voting system with robustness and universal verifiability. International Journal of Information Security. https://doi.org/10.1007/s10207-019-00465-8

[3] E. Elewa, A. AlSammak, A. AbdElRahman, T. ElShishtawy, "Challenges of Electronic Voting A Survey", Advances in Computer Science: an International Journal, vol. 4, no. 6, pp. 98-108, 2015.

[4] Aranha DF, Ribeiro H, Paraense ALO (2016) Crowdsourced integrity verification of election results. Annals of Telecommunications:1–11. doi:10.1007/s12243-016-0511-1

[5] Gjøsteen K, Lund AS (2016) An experiment on the security of the norwegian electronic voting protocol. Annals of Telecommunications:1–9. doi:10.1007/s12243-016-0509-8

[6] Budurushi J, Renaud K, Volkamer M, Woide M (2016) An investigation into the usability of electronic voting systems for complex elections. Annals of Telecommunications pp 1–14. doi:10.1007/s12243-016-0510-2

[7] Neumann S, Volkamer M, Jurlind B, Prandrini M (2016) Secivo: a quantitative security assessment model for internet voting schemes. Annals Telecommunication pp 1–14

[8] Ayed, A.B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017