EasyChair Preprint

№ 15282

Revolutionary Blockchain-Powered Voting System

P Velmurugadass, Andem Uday Kiran Reddy,
Ananthula Jeevan Kumar, Adabala Sriram and Athapakala Vignesh

October 22, 2024

REVOLUTIONARY BLOCKCHAIN-POWERED VOTING SYSTEM

P.Velmuragadas[1] , Andem Uday kiran Reddy[2] , Ananthula Jeevan Kumar[2], Adabala Sriram[2] ,Attapakala Vignesh[2]
[1]Assistant Professor, Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education, Krishankovil, Tamilnadu, India.
[2]UG Students, Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education, Krishankovil, Tamilnadu, India.
velmurugadass.p@gmail.com[1], udaykirana879@gmail.com[2],
ananthulajeevan@gmail.com[2]adabalasriram7@gmail.com[2], vigneshathapakala@gmail.com[2]

1. ABSTRACT

E-voting made the elections somewhat cheaper and convenient than the pen and paper method it was considered to be untrustworthy because anyone with physical control over the system could disable it and manipulate the results. Having a central electronic system is also paramount in the process, such as e-voting, result stream, and results as well as outcomes. The electorate is not fully protected owing to the ease with which voters can be reached. Moreover, it threatens free and transparent election, as well as the right to vote. Mobile voting presented in this study allows to get rid of the nuisance connected with traditional elections through the application of the relevant technology, blockchain which has become rather interesting for a number of applications because of the unique characteristics which make it different from the competitors. The purpose of this research is to design a distributed, not a centralized, municipal electronic voting system through BaaS for the protection of voter identities, the privacy of transferred data and the ability to check the outcomes of the voting process based on the principles of decentralization.

KEYWORDS: E-Voting, Blockchain, Smart Contracts, Ethereum Cryptocurrency.

2. INTRODUCTION:

An election is the process of voicing support for a particular candidate to be elected. an official post to secure an official post for the purpose of holding directly through the voters towards the government. Elections are considered asone of the principles on which any democratic society was founded in the first instance the citizens vote for the competent so as to make a decision.any given candidate to form what I would like to call a 'healthy' democracy. The history ofelectionoriginated from ancient Greece, Rome, and throughout the medieval. For a long time they elect the pope and the holy roman emperor. In India it has its origin from the earliest stage of the Vedic civilization when the king was elected by the people. The modern day elections arose only after the middle ages all over Europe as well as the North. America. The latest idea of voting process or electrical voting machinereplaced the conventional form of voting that was a boring operation for it requires strenuous and exhaustive work. makes it allow a wide range of margine of error and mistakes. With the techno-advancement, the mechanical system of voting was much more fluent, Functional and minimized the human. effort, and thus makes the work more reliable and accurate. The suggested system makes uses of the kind of technologies such as e-voting,from the prospects of the point mentioned above There will be more security from the use of blockchain and smart contractconvenience.

E-Voting:

E-voting is defined as the means by which an individual can vote, and also the manner in which the votes cast are tallied. Votes through an electronic systems. Votes are stored in tapecartridges, diskette, smart cards and sent to a centralizedplace where compilation process took place. The various forms of e-voting are DER (direct electronic recording) touchscreens, optical scanners. The two basic chronic classifications of e-votingare:Electo-Voting System to involve the use of electronic voting machines at any given electionrelocated to the polling boots with someelection administrator who will oversee the voting exerciseand people have to stand in a line for the purpose of voting.

Remote e-voting; where the individuals concerned do not have to be physically present at thepolling station instead can vote from

anywhere they want throughdestination using computer, mobile phones etc.Whether we like it or not, elections have to be secure and beyond reproachof theorganization. Citizens' voting has to be protected and they should also be protected from publicity but counting should not be lengthy as it raises concerns.

Blockchain:

In this case, Blockchain was a substitute to the traditional modeling approach by making the system unalterable and transparent. Blockchain is an ordered data structure; a block in the blockchain is connected to each other in the chain. The first block is termed as the generation block. Every time a new block is received a stack of blocks known as a blockchain will be created. Simply, it is composed of field data, field hash and field 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 invalidatesthis block and all other succeeding blocks herein. This is to avoid tempering, because making change in one block you will need to calculate hash for every other following block, however hackers these days can compute hundreds of thousands of hashes in a matter of seconds. To overcome this problem it makes use of proof-of-work concept which slow-down the rate of formation of a block. In addition it make use of a distributed peer to peer network where there is no place present in the middle of it. When a new block is generated it is broadcasted to all other nodes in this network each node has to check whether any tempering has been done with the help of block chain and after getting the positive response from each node the block chain is added to other block chain. The network or chain results in the making of consensus on whether the block is valid or not in which blockchain is so secure safe and reliable.

Smart contract:

A smart contract is an application code written on a blockchain that executes terms of the agreement between two or more parties. incorporated in a blockchain administrative computer code. This code consists of a number of norms regulating the interaction and the outcome regarding the contract between the parties the will be upheld by operation of law once the already defined rules are met. Smart contract provide a blueprint to follow on. efficient control between two or more parties of tokenizes assets and access rights. Blockchain is just a reference list that cannot be changed, without relevant contract, which enlarges and builds out the potential of blockchain technology.

In smart contract, the conditions are verified through self-verification. by data interpretation. Every node of the networks will ensure the success of fulfilling a single contract, which relieve the contract prevents contractual counterparties and other creators from monitoring the fulfilment of the contract. Smartcontracts are automatic and the covenants ofthe agreement of different parties are hard coded into the system. What this means is that legal duties can be documented by means of smart Even limited contracts can be transformed into an automated process. The execution of the contract can be automatically triggered by a field, for instance, expiration date.

In this paper, the concept we choose to deploy is the blockchain based e-voting system. that eliminates the difficulties which are associated with e-voting and helps to develop credibility for the people in order to vote with integrity. Moreover, it will also be a useful move toward the creation of smart governance.

3. LITERATURE REVIEW:

This e-voting system was better than the conventional use of the pen and paper voting system in several waysand paper approach and were adopted in many a organization during and after the intensitycountries. Many nations implementing the e-voting system in their election process. Despite many benefits it brought to the tableas for example, higher voter turnouts, auditability of results, low cost and convenient.Inclusiveness of the society, free and fair elections, etc. but common was several crucialthat includes opportunities, risks, threats and other factors pertaining to the

implementation of EDI and also several challenges and issues that may affect it.

In a study by Abdelwehab et al the authors highlighted a few problems of e-voting system that is the legal problems, barricade social and cultural processes, technical barriers, assaultsetc.

Theant before elated Diego F. Aranha et al. in their work found an use political experiment to check the credibility of the election results and to improve the openness and electorate engagement in the electronic elections. This proposal was based upon two subsequent proposals which were more fully developed and presented with greater detail the next day. aspects i.e. distributed collection of pole tape, made by mobile devices from the voters and crowdsourcing election data Saad Moin Khan et al.From the electoral authority a process such as verification has to be undergone.According to our previous work, Kristian Gjosteen and Anders Smedstuen which if voters make use of voting protocol correctly then it will also serve to eliminate all possibility of an attack on the outcome of any election. they provide a statistical approach for enhancing the security of e-voting.

Budurudhi et al tries to explain how the concept of developing can be appropriately approached. voting machine interfaces for enhancement of role of electors and survey administrative and then use the outlined interfaces for complex elections. The process of delegating a complex and major business activity, such as manages, to a remote location creates the following issue:as the voting device is reported to be strongly associated with the interface. which in turn determines votes as confirmation of voting is an important issue. Much of the work in remote–As much as with electronic voting cryptography voting are involved. structural design and verification to protect the desired property.

In this respect, Neumann et al. affirms that for one to be specific, then he/she must posses specific thought. advice on which type of voting system would suite the country best fit to that particular context, on that basis they named a model for the analysis of how the electoral's voting schemes work. context and the model has been used to settings the context of Estonian internet voting.

Cause as there were many issues with electronic votingespecially on physical security aspect where there was a recorded improvement across the three organizations. Samir Ahmed Ben Ayed his work identifies on how sort of leverage the advantages of the blockchain technology in the processterms pertaining to e-voting intended to make the process safe, secure, anonymous etc.Hsiao, Jen-Ho et al in their contribution also employ the smarts on: of decentralised block-chain contract in e-votingto involve all the voters in assessing and in making the marks on the ballots. It enhance the confidence of the electorate and reduce the…misuse of election capital.Jonathan Alexander et al.in their study adopted the identification of NetVotefor user interface of the program it employs decentralized application. The dApp admin assists the electoral administrators on how to determine electoral policies, create voting, register policies. voting starts and voting ends. Voters are first identifiedby other applications of the technology such as biometric reader services. To test and checkwhere the results of election TallydApp is used. This NetVote reinforce three kinds of elections: private election, open election, The token holder elections.

Of course, there are many problems in current e-voting system which acts as a hindrance in accomplishing the accurate results like:

a. Prone to hacking.
b. Inefficient auditing
c. Confusion of voters' intentions.
d. Political biasness in a manner that is in favor of the manufacture.
e. Stressing of the affairs in software programs.
f. Lack of efficiency in the consolidation of the casted votes.
g. Hardware malfunctions, etc.

The main finding of this research will be the general objective of creating an electronic voting system which is based on the perfectly adopted blockchain technology that solves the not a new issue for legislation. This model can be has been practiced at different levels which may be school

level, college level, in general buildings, schools, shops and even at national level voting. Because elections are offices that are always facing some of the fraudulent practices like espionagemachine, changing of votes, organizations of information campaigns and more. All of these problems will be contrecoup by our model

4. METHODOLOGY:

The proposed system incorporates the following tools as specified below GANACHE The following tools are used for developing smart contracts, Truffle framework, npm, and Metamask. Truffle imports the smart contract in the blockchain though as Ganache manages

The internal blockchain and it will be accessed by usingmetamask. Some Ether is in otherwords Ethereum's digital currency is needed by a user for an account with wallet address. To write As for the transaction to blockchain, the user requireds to pay a certain transaction fee which is known as gas. Once votes are cast the process is done by many nodes on the network called as minners. These miners are very much in a rivalry against each other in order to complete the transaction. The successful single male miners included Those who are very serious in their job [(mining)], able to amass considerable size wealth [wealth established through mining], and strong ardent devoted [physically fit and sexually active]. transaction is rewarded with ether that users pay to vote. Instead of and at this very node we will be using ganache software for mining or to be precise for simulated mining.

New E-Voting System that has be developed:

Blockchain Preliminaries:

I argue that, in order to put our proposed model into practice, operating system should be 64- bit.

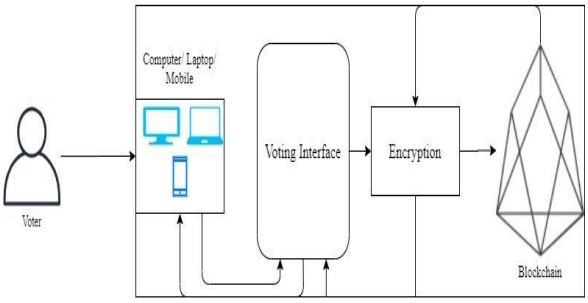
hardware/ machine, Recommended OS and above, NMP requirements.

Ganache, Metamask, solidity toolkit, Truffle framework.

1. Dependancy NPM(Node Package Manager)
2. Truffle framework
3. Ganache
4. Metamask
5. Programming language; solidity, HTML, JavaScript and CSS

NPM (Node Package Manager):

NPM is package manager that allows users to manage, install, update or it removes the node.js packages in an application. It is a command line based tool. It operates in two modes: local mode Appropriate: An Analysis for the Performance of Decentralized Blockchain E-votingand global mode. As for the global mode all node.js application are affected and in local mode only a particular directory in an application gets affected.



Truffle framework:

Truffle is just a fantastic application and can help in working with ethereum smartcontracts. It is for compilation, deploying as well as link of

Smart contracts, offers a testing application for automated manages parties, RFPs, contracts, networks and packages and etc.

Ganache:

Earlier it was called Testrpc and is available in two typescommand line and UI. A virtual blockchain creates testandard Ethereum addreses from all and key privatefiring a hundred ether each and preloading them with simulated hundred ether each. With In ganache there is no

mining rather its just approves transactionsevery transaction. To the extent that it is beneficial for operating systems such aswindows, Linux and mac.

Metamask is an open source, easy to use interface which has theIt is a type of operating system for graphical userinterface for doing transactions in ethereum.Ethereal Dapps can run without the full version of Ethereum node teaching your system browser. Metamask is essentially aintermediary between browser and blockchain ethereum.

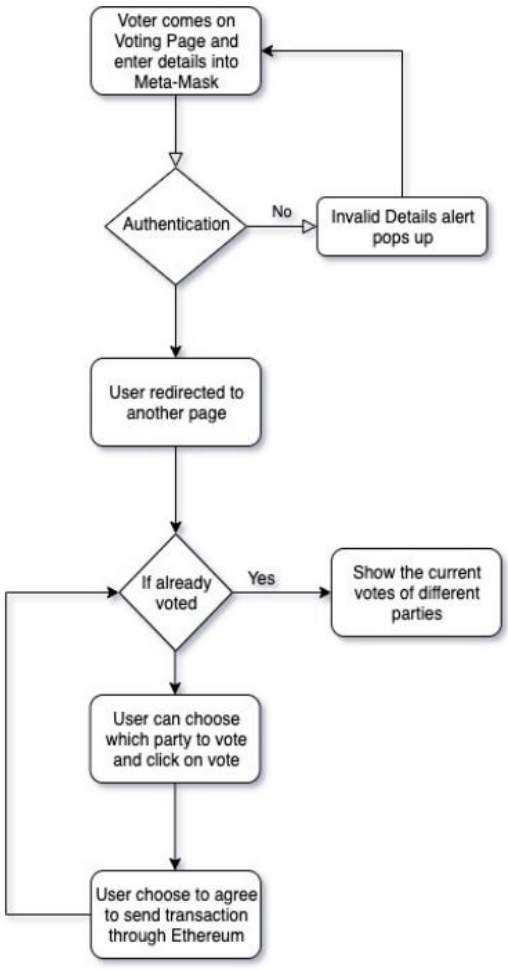
Solidity:

Similar to JavaScript, Solidity is a high-level language which completely supports contract-oriented programming.for contracts. It is a method of creating EVM machine level code and converts into simple instructions. It has fourvalue types namely: Boolean, Integer, Address and String yetis expressed by same operators as that of JavaScript.

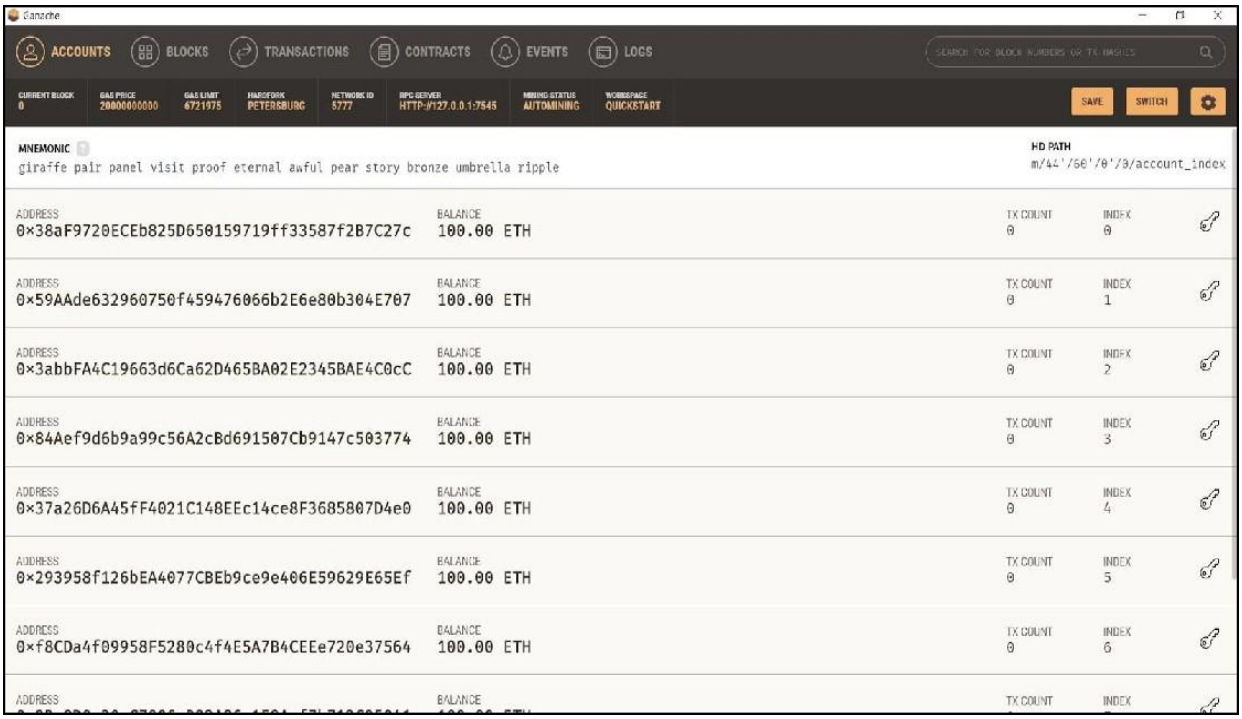
Working:

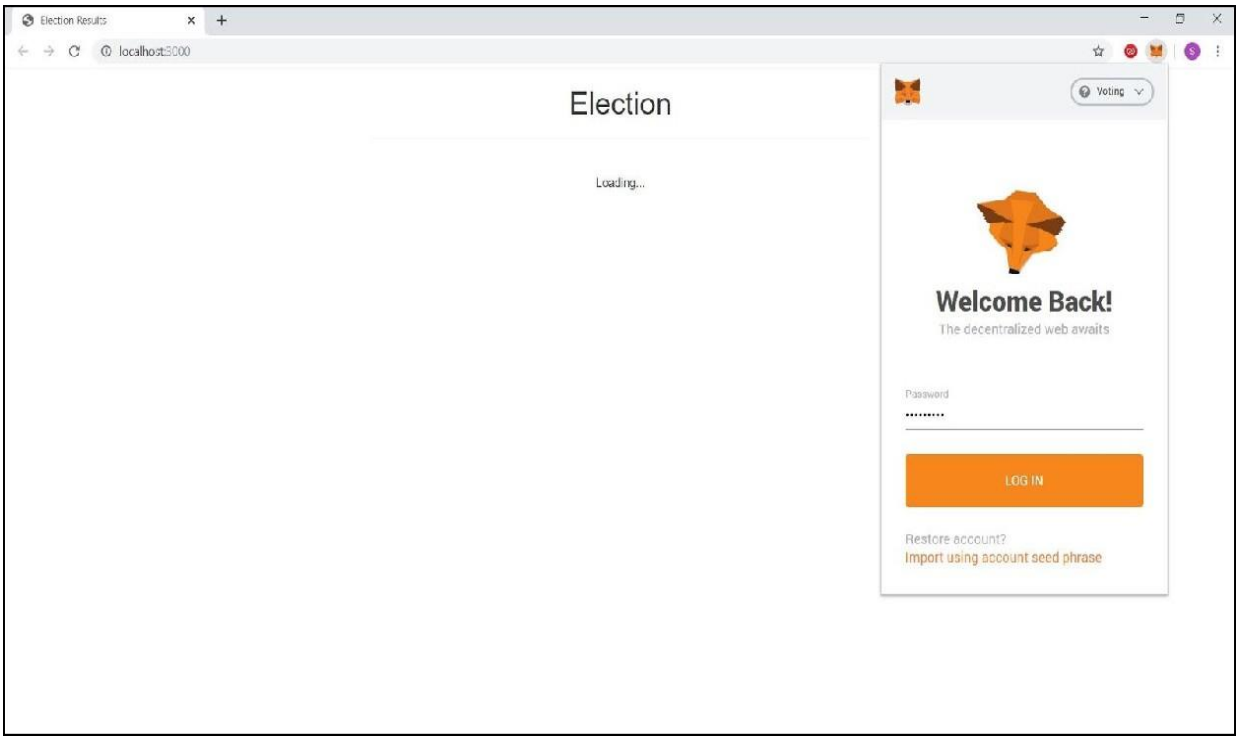
The voter can log on to the voting website, then he has to log in with the Chrome Extension of Metamask to interact with the local blockchain. When connection has been established, the page is updated the list of the candidates and what the current opaque entrega looks like to the user. votes. On that is the ability to vote within that ballot to select the candidate to vote for, if the voter chooses the candidate and click on vote, a metamask occasionally shows a pop-up which informs the Ethereum transaction that has to be made, one the user clicks on Vote, he or she gives a vote. the selected candidate so that the voter has not cast his or her vote before. If the user has voted the voting is disabled and the following message is displayed 'You have already voted!' once more, a failed transaction will take place and vote will not taking place.accounted.

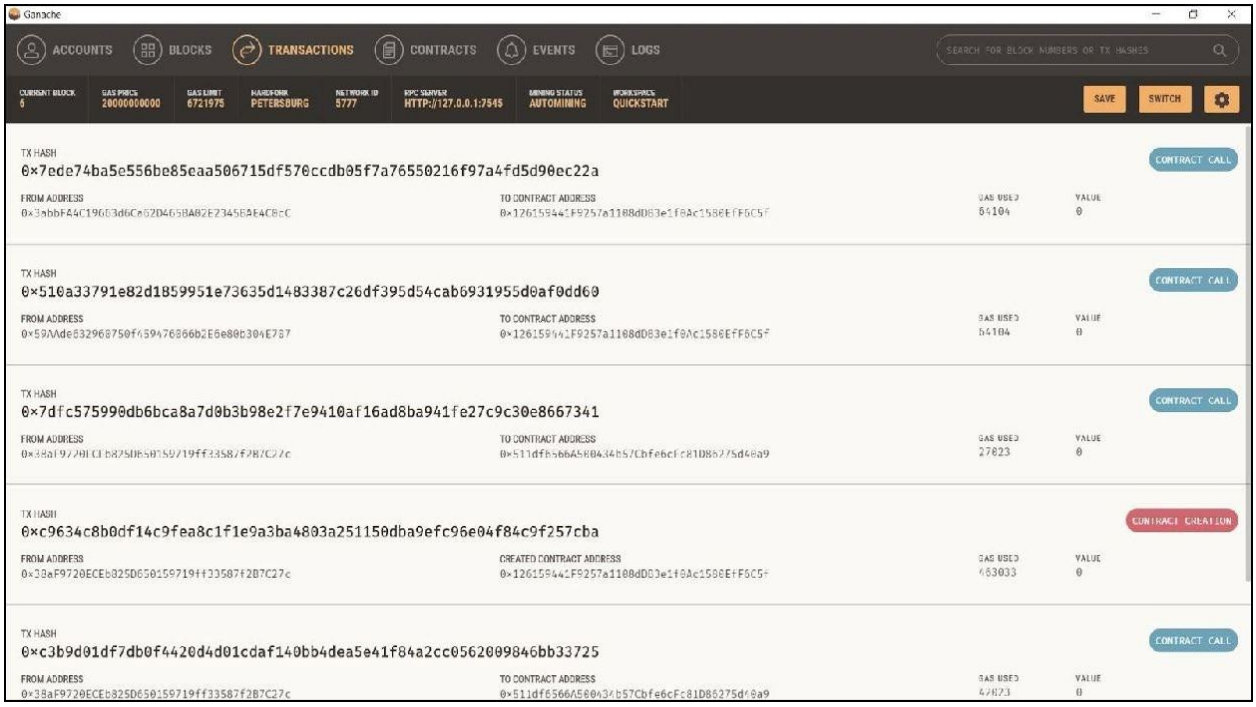
A Ganache is used locally to deploy the blockchain. ethereum is ready to interface with it and so is metamask. Truffle framework enables to transfer the smart contracts designed on solidity to the local blockchain. Whenever the user clicks to vote, metamask lets transfer Ether from one wallet to another. Every user is assigned a number, which is known as the Ethereum Address and Ethereum private funds and an exact amount of Ether where key is sent to all the voters' accounts. When the user votes, the Ether is then transferred from voter's account to the Candidate's account and all the move through blocks, then all the transactions will remain transparent to everybody once we commence the project. This will provide voters full openness and then they can verify. their votes. After the user will have voted the address will not. hold the same number of Ether, thus if the user tries they can choose to vote again, it will not be effected for the transaction and the vote will not be accounted. Mining is carried out by all the other nodes but here, we have authorized Ganache to automatically mine on behalf of other nodes.

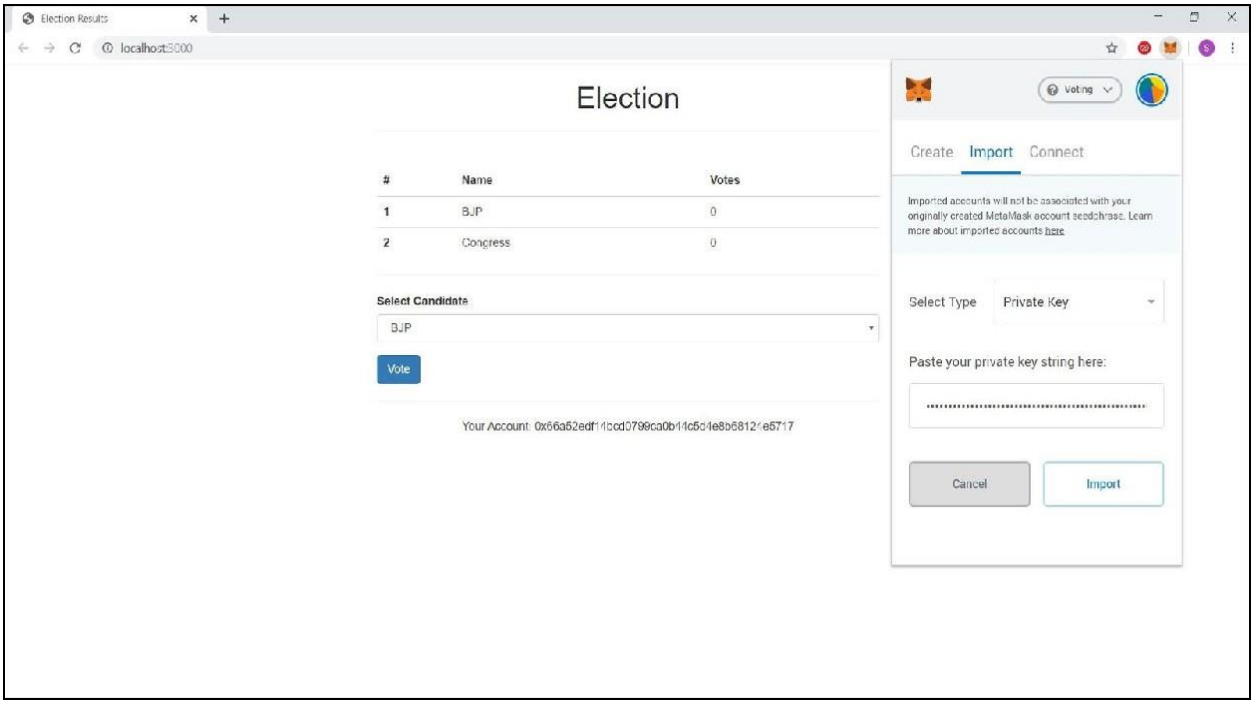


5. RESULTS AND DISCUSSION:






Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 6
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK PETERSBURG
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART
SAVE
SWITCH
TX HASH
0x7ede74ba5e556be85eaa506715df570ccdb05f7a76550216f97a4fd5d90ec22a
CONTRACT CALL
FROM ADDRESS
0x3abbF44C19683d6Ca62D465BA82E2345EAE4C8cC
TO CONTRACT ADDRESS
0x126159442F9257a1188dD83e1f0Ac1588EfF8C5f
GAS USED
64104
VALUE
0
TX HASH
0x510a33791e82d1859951e73635d1483387c26df395d54cab6931955d0af0dd60
CONTRACT CALL
FROM ADDRESS
0x59AAde832968750f459476866b2E6e80b304E787
TO CONTRACT ADDRESS
0x126159442F9257a1188dD83e1f0Ac1588EfF8C5f
GAS USED
64104
VALUE
0
TX HASH
0x7dfc575990db6bca8a7d0b3b98e2f7e9410af16ad8ba941fe27c9c30e8667341
CONTRACT CALL
FROM ADDRESS
0x38aF9720ECEb825D65015971 9ff33587f2B7C27c
TO CONTRACT ADDRESS
0x511df6566A58043 4b57Cbfe6cFc81D86275d40a9
GAS USED
27823
VALUE
0
TX HASH
0xc9634c8b0df14c9fea8c1f1e9a3ba4803a251150dba9efc96e04f84c9f257cba
CONTRACT CREATION
FROM ADDRESS
0x38aF9720ECEb825D65015971 9ff33587f2B7C27c
CREATED CONTRACT ADDRESS
0x126159442F9257a1188dD83e1f0Ac1588EfF8C5f
GAS USED
463033
VALUE
0
TX HASH
0xc3b9d01df7db0f4420d4d01cdaf140bb4dea5e41f84a2cc0562009846bb33725
CONTRACT CALL
FROM ADDRESS
0x38aF9720ECEb825D65015971 9ff33587f2B7C27c
TO CONTRACT ADDRESS
0x511df6566A58043 4b57Cbfe6cFc81D86275d40a9
GAS USED
47823
VALUE
0


Election Results
localhost:3000
Election
Name Votes
1 BJP 0
2 Congress 0
Select Candidate
BJP
Vote
Your Account: 0x66a52edf14cd0799ca0b14c5d1e8b5812e6717
Voting
Create Import Connect
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:
Cancel
Import

6. CONCLUSION & FUTURE SCOPE:

The modern concept in the area of voting system is the following: Blockchain technology which has time andagain been shown to be time and; is cheap but is also secure, hence is more than the previous conventional methods were more accurate and less ambiguous, But now we have reliable and precise one. In this paper In this paper, we have utilised blockchain based e-voting with smart that contain the framework of rules of the real time communication and decision on the contract between parties. Some of the tools used include Ganache, Truffle framework, NPM and another package.

For implementation purpose, Ethereum and metamask were used. Asblockchain is a decentralized technology becauseThe current and significant changes as well as tempering in such system is quite possible. The system proposed will offer convenience to the voters in the following waysenabling them to plug into the system with friendly interfaces voting, by means of the user interface which is the only method accessible to them. they can import their account and can easily get their vote reviewed. It developes an impression of confidence to the voter that their vote counts calculated and stored in a securely

7. REFERENCES:

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

[2] Zhang, S., Wang, L. & Xiong, H. Int. J. Inf. Secur. (2019) Chaintegrity: 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] BudurushiJ, Renaud K, Volkamer M, WoideM (2016) An investigation into the usability of electronicvoting systemsforcomplex 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 assessmentmodelforinternetvotingschemes. AnnalsTelecommunicationpp1–14

[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

[9] HsiaoJH,TsoR.,ChenCM.,WuME.(2018) Decentralized E-Voting Systems Based on the Blockchain Technology. Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore.

[10] JonathAlexander,StevenLanderanBen Howerton(2018).Netvote:ADecent.