Decentralized Application on Voting System

P. Sri Subhash, K.Kiran Kumar, R. Goresh Chowdary, B. Sai Teja,P.S.G.Aruna Sri

Abstract: Election is a significant job in our Elective Government. As technology progress with upcoming days, its impact becomes more optimistic. One such outcome is the Blockchain. It is possible to transform the process of voting system due to its decentralized property of immutability. Voting in most places are non-transparent and common with the corruption. In this paper we proposed the technology, is Blockchain technology. The concept of this paper is to develop a decentralized application for voting system. From there, the transaction votes are stored in the blockchain could be illustrated by the examining the block hashes. The outcome of the project shows the transaction of tokens from voter's wallet into the candidate's wallet. This application can deploy on a test platform using the Ethereum Virtual Machine (EVM) it provides the network to test the application. From there, the integrity of the blockchain technology is illustrated.

Keywords: Blockchain, Decentralized, e-voting, Ethereum, Smart Contract

I. INTRODUCTION

Blockchain is a mutual, conveyed record on which exchanges are carefully recorded and connected together with the goal that they give the whole history or provenance of a benefit from a product engineer's point of view. A blockchain is only a monster Merkle tree where each new node implants the hash of the past node just as the root hash of the present node activity, in the end framing a chain of hash-nodes. It may be not self-evident, however such a Merkle tree structure doesn't require a focal server. Members can perform exchanges without the requirement for a focal affirming authority. Potential applications incorporate support moves, settling exchange, casting a ballot and numerous others. The as of now well-known Voting frameworks depend on the outstanding customer server design. Blockchain then again is a developing innovation that furnishes arrange decentralization with no single purpose of disappointment and guarantees information unchanging nature through cryptography and use of proof of work protocol.The Ethereum Blockchain is an open-source appropriated registering foundation of Turing-complete scripting language in which programming designers can deploy decentralized application. We can likewise know as the D-application. We have some development periods of the blockchain innovation.[1]

Revised Manuscript Received on November 25, 2019.

P.Sri Subhash, Scholar pursuing Electronics and Computer Engineering from KL deemed to be university.

Dr.K.Kiran Kumar,Professor,Department of Electronics andComputer Engineering, Koneru LakshmaiahEducation Foundation, Vaddeswaram, AP,India

R.Goresh Chowdary, Scholar pursuing Electronics and Computer Engineering from KL deemed to be university.

B.Sai Teja, Scholar pursuing Electronics and Computer Engineering from KL deemed to be university.

P.S.G.Aruna Sri Associate Professor,Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

This is done by applying the concept of blockchain that brings with it a considerable amount of added security and transparency to the current system. The decentralized and distributive nature of blockchain are the key features on which the whole system[3]
Is based upon. Furthermore, the immutability of the system ensures that there is no scope of tampering as any and every transaction that has been recorded has been done so permanently.

II. EXISTING SYSTEM

Electronic Voting:

Electronic voting system is an electronic device which is used to cast and count the votes. This system is directly operated by the EVM (Electronic Voting Machine). Some process is held in the elections. Voters will enter their detail information into the e-voting system. The system will validate the information of voters after voter will cast their votes through the ballots the votes will stored with security then the system calculates the votes and final decision is announced.[6]
In Generally, there are two types of e-voting:

1. Electronic Voting (e- voting) it is supervised by election authorities in polling booths.
2. Remote Voting (i- voting) here the voters will cast their vote through online from any location.[4]

Documented problems with e- voting:
Estonia:
Estonia is first nation to introduce the online voting system in 2005. The voters will cast their votes through internet they should download the voting application and validate their identities of their ID'S. later they found the system creates the problems with transparency and security.

III. PROPOSED SYSTEM

The current existing system is not good enough for efficient voting. The voting system here must satisfy following requirements-

1. The votes must be transparent and can be verified by anyone.
2. The voter information must be recorded correctly.
3. Only registered voters must be allowed to vote.
4. The voting system cannot be compromised by any hackers.
5. The votes once stored should not be changeable.

By using block chain, the following requirements should be satisfied-

1. Accuracy-In voting system, every vote must be recorded permanently so that it can't be duplicated or changed.

2. Authentication-Only registered people should be allowed vote. The system should verify voter's information in database before allowing any voters.

3. Anonymity-Voters personal information must be secured during voting.

4. Verifiability-Each vote must be verifiable and should be counted correctly.[4]

These security requirements are fulfilled by using –

A. Hash functions: The security and integrity of blockchain is maintained by using hash function. Hash function converts

normal text to hash value which cannot be read by humans. Each block in a block chain is processed one by one where a hash from previous block is connected. For accepting any block, it must have

correct hash value from the before node.[4]

B. Digital signature: It provides security for accessing voters information in voting.every signature will have private key and public key.private key used for accessing information and public key used for doing any transactions.[4]

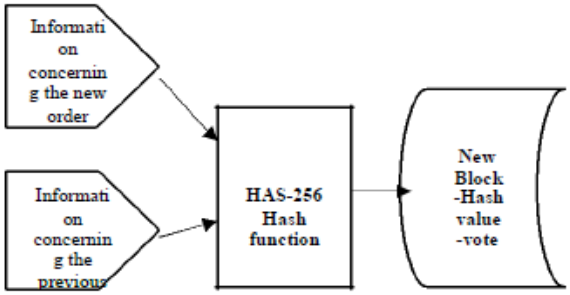


Fig1.Linking of nodes using hash function

IV. SYSTEM ARCHITECTURE

Blockchain was first presented by satoshi nakamoto, who proposed distributed installment framework that permits money transaction without any third-party financial institution. Bit is the first application of blockchain concept to provide secure transactions.[9]

Blockchain is a distributed, decentralized and immutable public ledger. Mining is the process that includes new block to blockchain. Miners use POW (proof of work) algorithms to add any new blocks to blockchain. In this algorithm miner will broadcast this block to the network, other nodes will verify correctness of the block and transaction it contains. After the verification block will be added to block chain. There are several types of Blockchains depending on the situation and requirement-

1. Permission less Blockchain – It is a public version of blockchain where anyone can be a user, and anyone can read/write a node. Its transactions don't require any permissions.
2. Permission Blockchain – It is operated by admin or stake holder. Only allowed users can see the transactions unlike public. Anyone allowed can do transactions here also.
3. Private Blockchain – It is a special type of blockchain controlled by one entity. These types can be used for transactions within organization.[1]

In the Proposed System, we will use Dapp (Decentralized application) developed using public blockchain. The frontend of a decentralized application is what you see it's a simple interface like a website or app. It is developed using HTML, CSS and JavaScript. Backend of Dapp is one or more smart contracts which contain some logic. Smart contracts are integral building blocks of decentralized application. Smart contract is developed using solidity language.

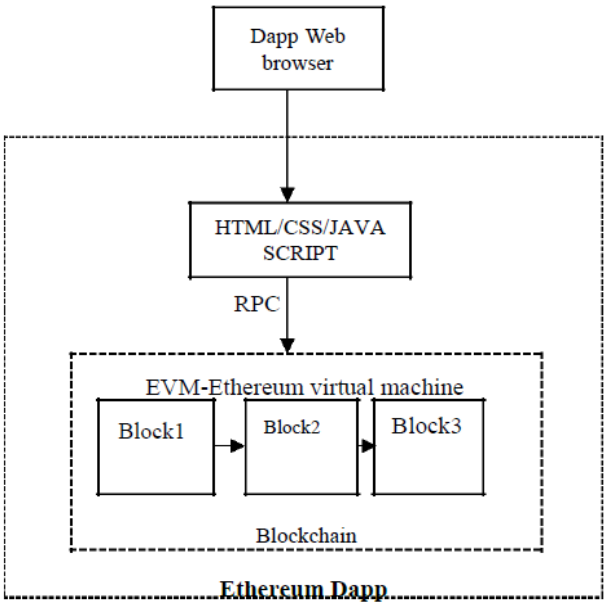


Fig2.Ethereum Dapp architecture

V. IMPLEMENTATION

This implementation consists of:

A. Frontend:

The frontend provides an interface to the users to access blockchain data and provide some inputs to blockchain. It is developed using HTML/CSS and JavaScript. Pages in frontend are as follows

1.interface is provided by Google Chrome and Metamask plug-in.

2.One HTML/CSS page

3.One JavaScript page

B. Backend:

1.Two smart contracts codded in solidity.

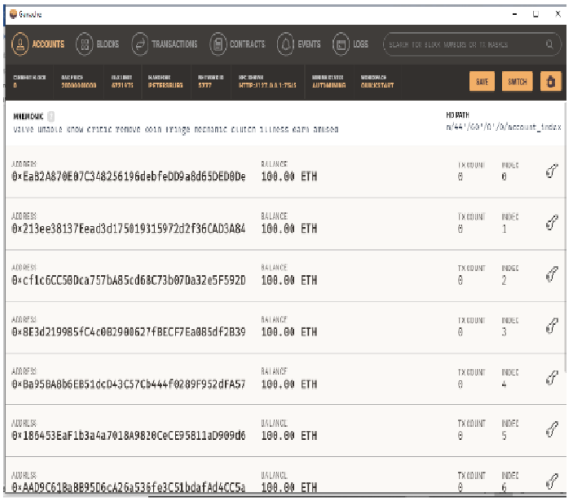
2.Truffle suite (Ganache) provided a modifiable Ethereum blockchain.

C. Metamask:

Metamask is a Google Chrome plug-in designed to make use of Ethereum browser without fully installation of Ethereum blockchain. It is used to manage decentralized applications, digital wallets and smart contracts. Metamask with web3 together ensures security while performing transaction.[11]

D. Truffle suite (Ganache):

Ganache is a personal Ethereum blockchain which can be used to issue and execute commands, testing and to perform transactions in blockchain. It is shown in fig3.[11]



Index.html-

It is a webpage for interacting with blockchain data. Used for buying tokens and voting with the tokens. everyone must buy a token to vote to a candidate and each time only one token can be purchased. This page will also be used for displaying number of votes and also voter information regarding tokens and votes he/she casted.[9]

App.js-

This JavaScript file will perform calculation required in voting like number of votes casted and tokens purchased by individual votes.

Voting. Sol -

This smart contract acts as a virtual ballot or voting. whole voting process code is written in this smart contract. This contract also verifies whether the voter is valid or not.

Migration. Sol -

This is a secondary Smart Contract file that maintains all the
migrations that occur each time the blockchain is reset and
restarted. It will also initialize count to zero when it is called.

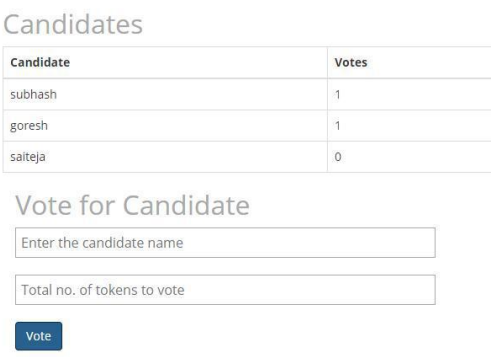


Fig4.user interface page

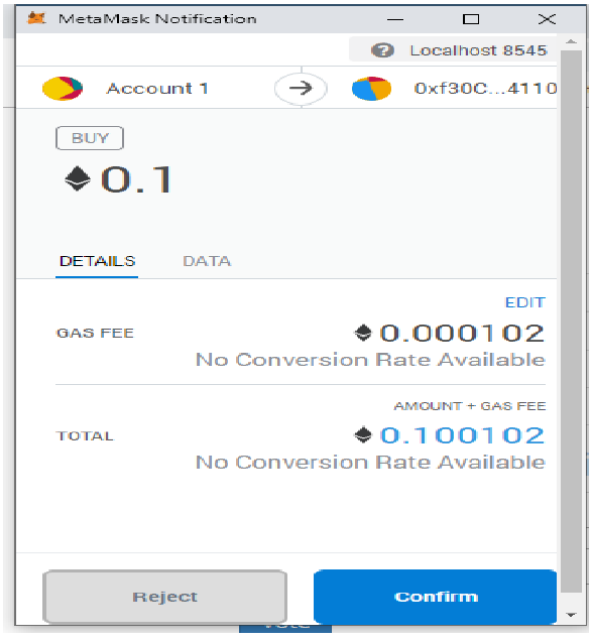


Fig 5 Transaction conformation in metamask

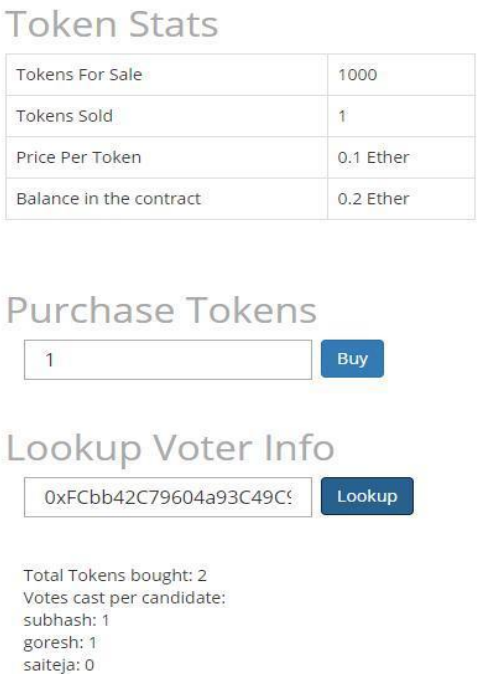


Fig 6.voter information

VI. CONCLUSION

The straightforwardness of the blockchain empowers to investigate and comprehension of races. By utilizing the Blockchain innovation it satisfies the exactness, verification, obscurity, obviousness. For e-casting a ballot to turn out to be progressively straightforward, and freely to investigate, a potential course of action would be base it on blockchain Technology.

This paper explosers the growing of the blockchain development and its usage finish in the law based plan.The blockchain will be openly certain and appropriated with the end goal that no one will have the choice to deteriorate.

REFERENCES

1. Rifa Hanifatunnisa, Budi Rahardjo 'Blockchain Based E-Voting Recording System Design', Bandung Institute of Technology, Bandung, West Java, Indonesia, 2017
2. Ahmed Ben Ayed, 'A conceptual secure blockchain- based electronic voting system', International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017
3. P.S.G. Aruna Sri, D. Lalitha Baskari,'A Study of Blockchain Technology', IJET (2018)
4. Clement Chan Zheng Wei, Chuah Chai Wen, 'Blockchain-Based Electronic Voting Protocol' University Tun Hussein Onn Malaysia, Malaysia, International Journal on Informatics Visualization (IJIV) Vol.2, No.4, 2018
5. Shalini Shukla, D.O. Shashank, 'Online Voting System using Ethereum Blockchain', IEEE (2018)
6. Harsha V. Patil, Kanchan G. Rathi, Malati V. Tribhuwan, 'A Study on Decentralized E- Voting System using Blockchain Technology', (IRJET) Volume: 05 Issue: 11 | Nov 2018
7. Pallavi Shejwal, Aditya Gaikwad, Mayur Jadhav, 'E- Voting using Blockchain Technology' , IJRAR December 2018, Volume 5, Issue 04
8. Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain – Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3
9. Shubham Pareek1, Anuj Upadhyay2, Satya Doulani3, 'E-Voting using Ethereum Blockchain', 2018 IJRTI | Volume 3, Issue 11
10. Nur Sakinah Burhanuddin, Fadhlan Hafizhelmi Kamaru Zaman*, Ahmad Ihsan Mohd Yassin, 'Blockchain in Voting System Application', 2018 IJET
11. V. Arun, Aditya Dutta, Sourav Rajeev, Rohan Varghese Mathew, 'E-Voting using a Decentralized Ethereum Application', International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-4, April 2019
12. Vurukonda N., Rao B. T, 'A Study on Data Storage Security Issues in Cloud Computing', Procedia Computer Science,Volume 92,Issue 132,2016
13. Vurukonda N., Rao B.T., Reddy B.T, 'A secured cloud data storage with access privileges', International Journal of Electrical and Computer Engineering,Volume 6,Issue 5,2016
14. Reddy V.K., Sushmitha Y., Rao K.T, 'Distributed authentication for federated clouds in secure cloud data storage', Indian Journal of Science and Technology 2016,Volume 9,Issues 19
15. Rathod S.B., Reddy V.K, 'Decentralized predictive secure VS placement in cloud environment', Journal of Computer Science 2018,Volume 14,Issue 3
16. Paruchuri V.L., Anantha N.L., Konagala V.L., Bhattacharyya D, 'Ciphertext-policy attribute-based encryption for access control of data in cloud', International Journal of Software Engineering and its Applications 2016,Volume 10,Issue8
17. Sahiti V., Raghava Rao K., Mohan Rao K.R.R, 'Hashing technique data optimization for low power consumption in wireless sensor network', Indian Journal of Science and Technology 2016,Volume 9,Issue 17
18. Jaya Rohit K., Siva Rama Krishna M., Geetha Krishna C.H., Aruna Sri P.S.G, 'Securing message at end-to-end mobile communication using cryptography algorithm', Indian Journal of Science and Technology 2016,Volume 9,Issue30
19. Noorbasha F., Manasa M., Gouthami R.T., Sruthi S., Priya D.H., Prashanth N., Rahman M.Z., 'FPGA implementation of cryptographic systems for symmetric encryption', Journal of Theoretical and Applied Information Technology 2017,Volume 95 ,Issue 9
20. Rama Satya Nageswara Rao I., Murali Krishna B., Shameem S., Khan H., Madhumati G.L, 'Wireless secured data transmission using cryptographic techniques through FPGA', International Journal of Engineering and Technology 2016, Volume 8 ,Issue 1

AUTHORS PROFILE

P.Sri Subhash is an Undergraduate Scholar pursuing Electronics and Computer Engineering from KL deemed to be university. He is working under the guidance of Dr.K.Kiran Kumar and P.S.G.Aruna Sri. His research interest includes cyber security and web technologies.

Dr.K.Kiran Kumar,Professor,Department of Electronics andComputer Engineering, Koneru LakshmaiahEducation Foundation, Vaddeswaram, AP,India His research interest includes cyber security and Bigdata.

R.Goresh Chowdary is an Undergraduate Scholar pursuing Electronics and Computer Engineering from KL deemed to be university. He is working under the guidance of Dr.K.Kiran Kumar and P.S.G.Aruna Sri. His research interest includes cyber security and web technologies.

B.Sai Teja is an Undergraduate Scholar pursuing Electronics and Computer Engineering from KL deemed to be university. He is working under the guidance of Dr.K.Kiran Kumar and P.S.G.Aruna Sri. His research interest includes cyber security and web technologies.

P.S.G.Aruna Sri Associate Professor,Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. She pursing Ph.D. from Andhra University,Vizag,AP,India. Her research interest areas are cyber security and cryptography