IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

Election system using Block Chain technology

Mayur Chaudhari

Student, Dept. of Computer, Shri sant Gadge baba college of engineering and technology, Bhusawal-425201, India

Abstract: Voting is an integral part of any organization which helps organizations to take important decisions after taking a consensus from others and help implement any idea/decision in a procedural manner. This system is an online voting system based on blockchain technology. In view of the problems of malicious voting, data security, privacy leakage and so on in the current online voting system, the system can guarantee the fairness, openness, verifiability and non-tampering of voting data in the voting system by combining the decentrization of blockchain technology, the non-tampering of data and the anonymity of the voting system. Users can use the system to create voting projects, set voting time, register to vote and other operations, the system also provides the voting data traceability verifiable function, designed to build a more efficient and safe voting environment for users.

Keywords: Blockchain, Decentralized, Security, Voting

I. INTRODUCTION

1.1 Existing System

Traditional voting systems like Ballot based voting have been around in the history of the voting process for quite some time [1]. The Kudavolai system used in village assembly elections in Tamil Nadu, around 920 AD can be considered as an example first use of ballots for voting. But the scenario took a different course during the 1990s where cases of ballot stealing, fake/bogus paper votes, booth capturing, etc. where reported, eventually leading to its downfall. The early 1990s saw the rise of electronic and digital voting systems which offered enhancements in security, labor work and integrity. These devices were made to prevent fraud by putting a limit on how fast new votes can be entered into the electronic machine and are currently used in many countries for their election processes. The first country to deploy electronic voting system for elections was Estonia which was soon followed by countries like Switzerland and Norway for their state and council elections respectively [2]. An voting system should be highly secured so that not only it's available to voters but also overcomes the challenges faced by current voting systems like tampering with the voter's ballot or changing votes. Many electronic voting systems currently claim to offer anonymity of voters by using Tor network but fail to hide voter identity as intelligence agencies often spy on the Internet and identify voters or intercept their votes.

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

1.2 Blockchain Technology

Blockchain technology was first proposed in the Bitcoin white paper in the form of a Proof-of-Work Chain. Blockchain is essentially a decentralized database, as the underlying technology of Bitcoin, blockchain is decentralized by distributed formula algorithm, the core of which is an open, programmable distributed database, which is global. Blockchain technology is not only used in financial transactions, but also to record everything of value in a wide range of applications, such as financial accounts, medical procedures, birth certificates, insurance claims, voting and anything else that can be represented by codes. In view of the problems of voting inefficiency, repeated voting, fraudulent ballots and security existing in the existing scheme, this paper puts forward the blockchain-based voting system on the basis of blockchain technology, and by introducing blockchain technology in the voting process, each voting data node can verify the authenticity and integrity of the voting ledger and construct history, so as to ensure that the voting record is reliable and uncorrected, which is equivalent to improving the accountability of the system and reducing the trust risk of the system. Block chain Technology helps to simplify the system as following

1. Tamperproof

Blockchain is the basic technology of Bitcoin, each data node does not need to trust each other, in timestamp, data encryption and other technologies based on the realization of decentralization, non-tampering and autonomy and other characteristics.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

2. Decentralized

The autonomy of blockchain determines that nodes in the blockchain network, will independently listen to other nodes occurred in the data information, and at any time to share, the entire process is the blockchain network independently realized, without manual intervention. Each node in a blockchain network is the maintainer of the entire network, and no node in the network has absolute priority power. This decentralized, distributed network structure is applicable to the voting system, the voting center does not need to maintain and manage the voting system and network, each user of the voting system jointly maintains and manages the information of the whole system, and can share the data information, ensuring the transparency of the network, but also to prevent malicious voting or tampering with fraud, fraudulent ballot fraud.

3. Trust

The block is created so that the cryptographic puzzle must be solved. Secondly, the computer that solves the puzzle, shares the solution to all the other computers on the network. This is called proof of work[5]. The network will then verify this proof of work, and if verified is then added to the network. The combination of these complex math puzzles and verification by so many computers, ensures that only a genuine block is added.

II. VOTING SYSTEM

All Blockchain-based electronic voting system is proposed to adopt C/S architecture, this paper according to the blockchain decentrization, node data sharing, node autonomy and so on, analysis of the electronic voting system, requires each voter to participate in the voting equally, after the voting is completed to generate a voting voucher message, after the message verification, the system broadcasts the voting record message to all nodes, all the nodes receiving the message update their own blockchain, store voting records, and jointly maintain the system voting history information. The following are the steps describing how the proposal works.

2.1 Login

The voter puts in his login information for logging into the system - in this case it would be using a 12-digit voter ID that is issued during registration, fingerprint and a onetime password (OTP) that is sent by the system to the voter's cell phone at the time of log-in. If the login data provided are correct, the user is granted to go to next window otherwise access is denied.

2.2 Cast Vote

Voters now come across the voting page that has all the details of the candidates taking part in the election, the user has to select any one candidate. User is prompted to confirm his voting as voting can be done only once. All this is done through a user-friendly website.

2.3 Encrypting Votes

As the voter chooses the candidate, it's time to covert to encrypt everything and convert it into a fixed length hash as our aim is to fasten the process of voting by converting variable length data that includes Voter Id, Voter account address, his credentials, vote that he has casted, etc. to a fixed length hash value for faster processing. This uses SHA one way hashing technique that cannot be reversed and is send for verification. SHA stands for Secure Hashing Algorithm. On getting a certain set of input char acters, this algorithm converts variable length input strings/integers into fixed size characters called Hash. It generates unique value for a given input and the generated function is of fixed size 256 bits (32 bytes)[7]. If an attacker attempts to retrieve voter information, he has to perform a brute force attack of guessing thousands of hash combinations that give back the voter account value, which is practically impossible. Hence encryption makes the process secure.

2.4 Adding vote to blockchain

Using protocols like consensus and proof-of-work, a block is added into the chain after validation.

III. SYSTEM DESIGN

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

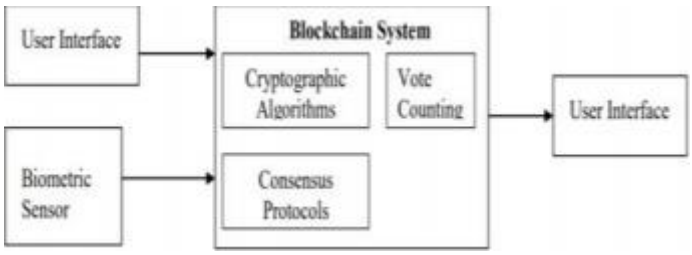

Fig. 1 Architectural block diagram of Voting System.

The above block diagram depicts the interaction between the three modules of the system. The inputs from webpage consists of user input data, signup and login details whereas the Biometric being the hardware interface provides the fingerprint of the voter. Inputs from both the modules interact with the Blockchain system that encrypts, verifies and validates the votes and provides a secure channel for the voting process. The results are then displayed on the User webpage.

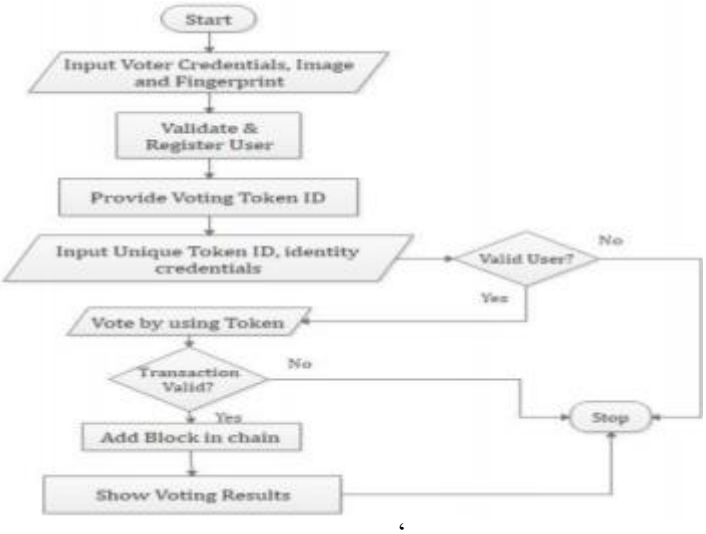

Fig. 2. Flowchart of the voting system

The above figure depicts the flow of the voting system. After voter sign in data and biometrics are provided, the user is validated and registered into the system. Each voter is provide with a unique 12 digit Voting Token ID (VTID). If the voter attempts to login into the system, he/she has to provide his/her identity credentials. If the details match es he/she is redirected to the login screen otherwise access is denied. Now while voting, if the VTID is provided wrong, the transaction is considered invalid and block is not registered. If it's legitimate, it is added into the system and live results are displayed.

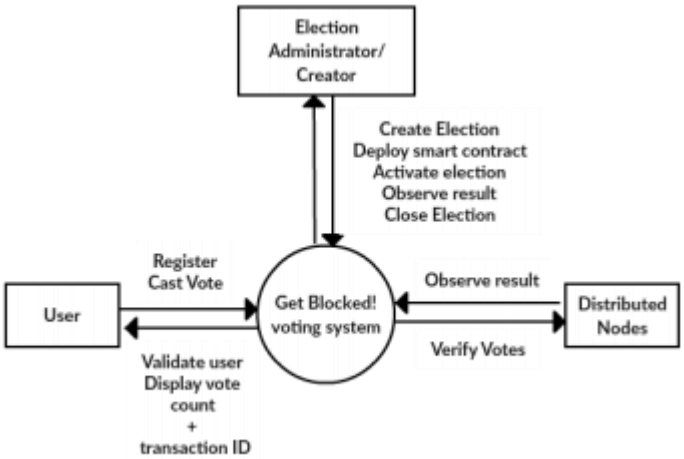

Fig 3. DFD level1 system design

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

The above dig illustrates A level 0 DFD, also called a fundamental system model or context diagram represents the entire software element as a single bubble with input and output data indicated by incoming and outgoing arrows, respectively.

IV. ALGORITHMS USED IN BLOCKCHAIN

Algorithm in block chain is used for the modification and validation of blocks. Con senses algorithm is widely used for the validation in block chain [4]. This algorithm further can be identified into Proof of work algorithm and Proof of Stake algorithm. Consensus algorithm is mainly used when there is any faulty or non-working node. It ensures that the information is transferred to all the nodes and blocks present. Single data value among distributed processes or systems is used to achieve agreement by Consensus algorithm process. Multiple unreliable nodes are involved to. With the help of consensus algorithm, we can reach out to every node. Which will help us to identify that the block added to the system is successful or not.

It is the inbuilt algorithm which keeps audit of all the blocks present. This helps the system to work without interrupt and flawlessly. Each and every block is audited as soon as the transaction takes place. Updating of blocks is also done by this algorithm. It prevents system failure due to any faulty block addition to the system. Each and every node is monitored as it gets newly add to the system. here due to this redundancy is reduced and every node is checked. Consensus also helps to prevent different types of attack like dos attack. As every block is added only after verification this makes to identify attack. Solving the issue, known as the consensus problem, is important in distributed computing and multi-agent systems. When node generates and transfers the data and consensus problem arises then BFT helps to overcome and make sure that the information in system is safe if issue occurs then liveliness occurs within [(n-1) ÷3], n is the number of replications occurs nodes can be handled up to 33%. 3F+1 faulty node can be handled. [7] Using the consensus algorithm N/2+1signature should be present to become the valid block into the system, where the N is number of signatures send by the commissioner [8]. Valid block generation can be called as round block consensus. The probability that we can find valid block is added is-

$$P(X) = \frac{N_c!}{X!(N_c-X)!}\left(\frac{K}{N_{bc}}\right) \times \left(1-\frac{K}{N_{bc}}\right) N_c - X$$

In order to make the results of the voting more impartial, it is hoped that the number of votes that a butler can receive exceeds Nc/2. So, it can be figured out the probability P1 that a candidate's votes can exceed Nc/2

$$P1 = \sum_{i=N_c/2}^{N_c} \quad \frac{N_c!}{i!(N_c-i)!}\left(\frac{K}{N_{bc}}\right)^i \times \left(1-\frac{K}{N_{bc}}\right) N_c - i$$

Poof work is the implementation of the consensus algorithm. Proof of work is the mystery that is to be solved if we find the correct way to solve the solution is not far. This is analogous to a solve the mystery. Effort is required to put the mystery solution together, but it takes only a momentary solution to see that if one has been concurred correctly. In Proof of Work consensus, the effort required to solve a mystery is called Work, and a solution is called a Proof of Work [9]. In other words, the solution to the mystery proves that someone did the work to find that solution. Blockchains which use Proof of Work algorithm consensus require exact proof to create new block and added to the blockchain. This is used to add new blocks into block chain. This Work is frequently referred to as 'mining.'

V. RESULTS

- Creation of blockchain account for storing the vote and user details.
- Creating the blockchain contracts for maintaining authenticity, and securing information.
- Sending of Ether to other accounts for validation of vote, successful addition of vote.

The screenshot of implemented modules is shown below:

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

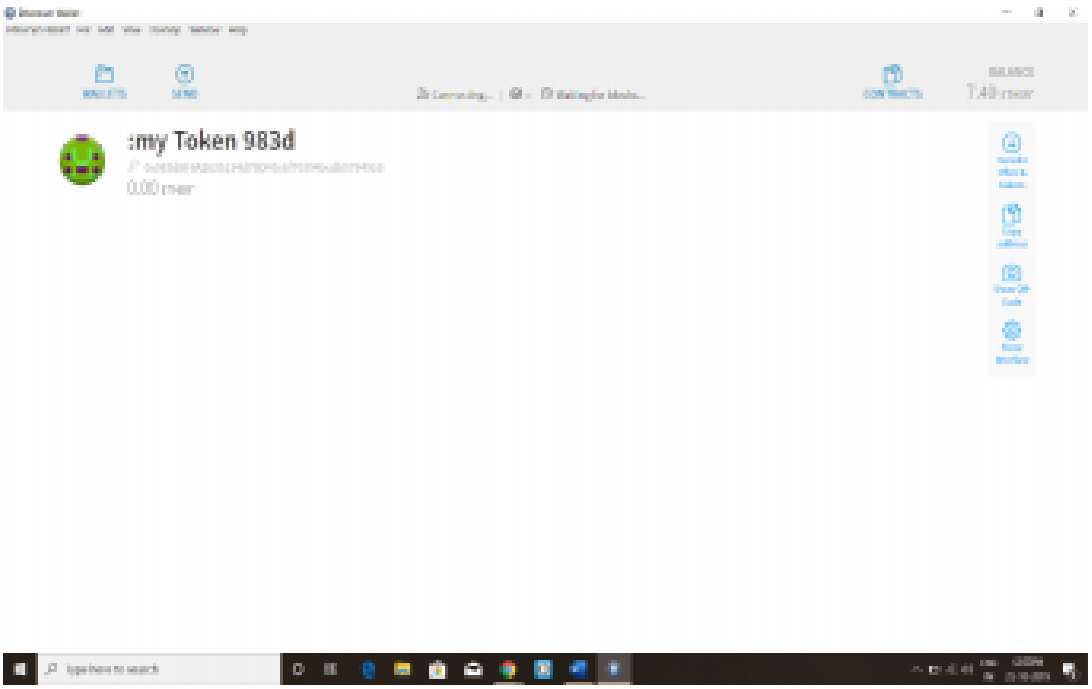

Fig4.Blockchain token for vote transfer

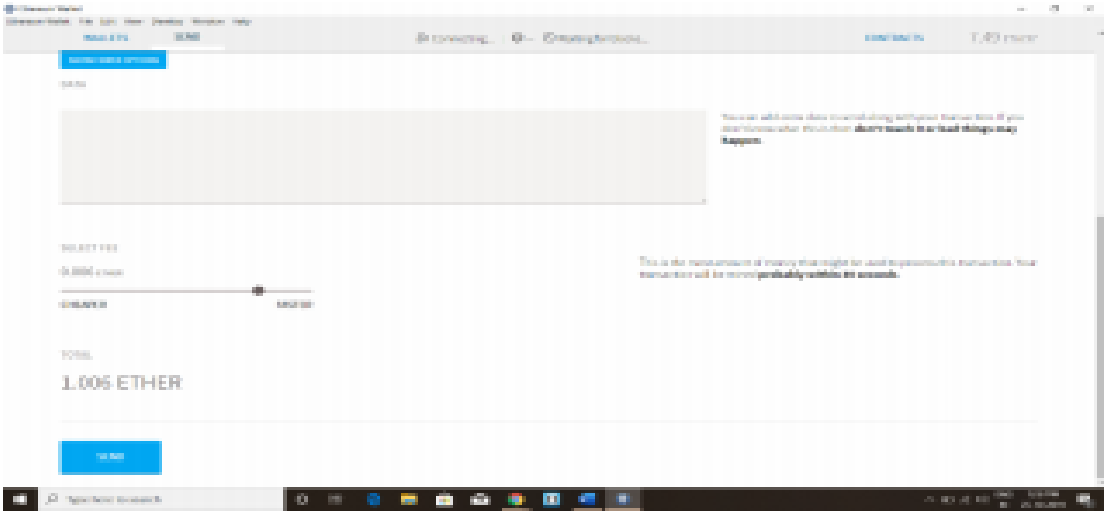

Fig5.Ether added to the account.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

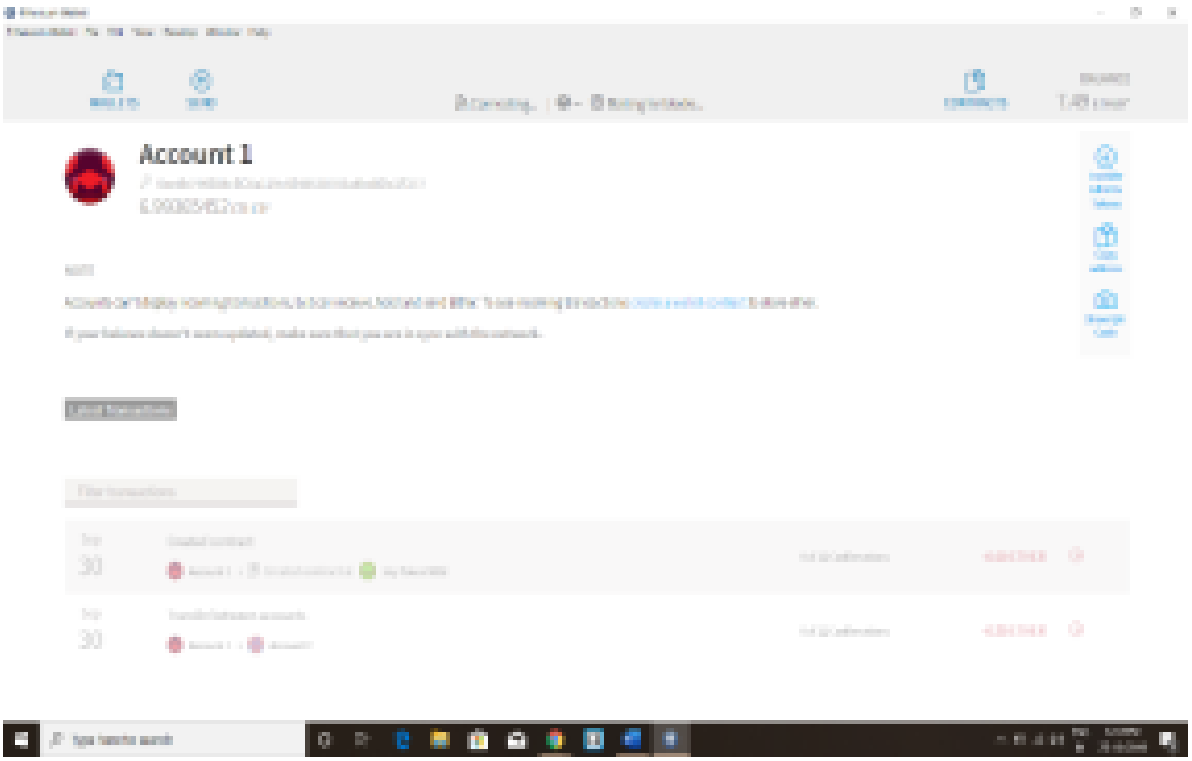

Fig6. Account showing number of total ether present

VI. CONCLUSION

E-voting is a potential solution to the lack of interest in voting amongst the young tech savvy population. E-voting is becoming more open, a potential solution would be base it on blockchain technology also transparent, and independently auditable. This system takes advantage of the transparency of smart contract to allow all voters to participate in both the recording and verification of Votes. It enhances the voters' confidence and reduces the waste of election resources. Blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

REFERENCES

1. Ahemadben International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017 DOI:10.5121/ijnsa.2017.9301 A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC.
2. 2. C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Elec tronic Voting Systems. arXiv preprint.(2017).
3. L. M. Bach and B. Mihaljevic"Comparative analysis of blockchain consensus algo rithms". Published in 41st International Convention on Information and Communica tion Technology, Electronics and Microelectronics (MIPRO)2018
4. Kejiao Li∗, Hui Li∗, Hanxu Hou, Kedan Li and Yongle Chen∗"Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain".Published in IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) 2017
5. Emre Yavuz, Ali KaanKoc "Towards secure e-voting using Ethereum block chain"Published in International Symposium on Digital Forensic and Security (ISDFS), At Antalya, Turkey, Volume: 6(2018)
6. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and VoterPrivacy(2018)
7. RifaHanifatunnisa and Budi Rahardjo"Blockchain based e-voting recording system design " Published in 11th International Conference on Telecommunication Systems Services and Applications (TSSA)2017
8. J. Gerlach and U. Grasser, "Three Case Studies from Switzerland: E-voting", Berkman Center Research Publication,(2009).
9. Sloane Brakeville, Bhargav https://developer.ibm.com/tutorials/cl-blockchain-basics- in tro-bluemix-trs/ PerepaPublished March 18,2018.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8540

10. https://en.wikipedia.org/wiki/Electronic_voting_in_India#Voter-rifiable_paper_audit_trail. 11. D. Ashok Kumar, T. Ummal Sariba Begum , "Electronic Voting Machine – A Review," in International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012)., TamilNadu, 2012.
11. Drew Springall, Travis Finkenauer, Zakir Durumeric, "Design of Distributed Voting Systems," 24 September 2015. [Online]. Available:
12. https://arxiv.org/pdf/1702.02566.pdf.
13. Andrew Barnes, Christopher Brake and Thomas Perry, "Digital Voting with the use of Blockchain Technology," 2016. [Online]. Available:
14. https://www.economist.com/sites/default/files/plymouth.pdf.
15. 12
16. Rishav Chatterjee, Rajdeep Chatterjee, "An Overview of the Emerging Technol ogy:Blockchain," in International Conference on Computational Intelligence and Networks, Bhubaneswar, India, 2017.
17. Gaby G. Dagher, Praneeth Babu Marella, "BroncoVote: Secure Voting System using Ethereum's Blockchain," in 4th International Conference on Information Systems Security and Privacy (ICISSP), S. Francisco, 2018.
18. Friðrik Þ. Hjálmarsson, "Blockchain-Based E-Voting System," in IEEE 11th International Conference on Cloud Computing, 2018.