IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 08-13

Blockchain based E-voting system in P2P Network

Miss.Vrushali Bapusaheb Bhusal[1] Prof.ManojWakchaure[2]
P.G.Student,Department of Computer Engineering Amrutvahini College of Engineering,Sangamner,MH,India[1]
Assistant Professor, Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner,MH,India[2]

Abstract: *Electronic voting (also known as e-voting) refers to voting using electronic means and to take care of the votes given by the user and counting the votes accurately. An e-voting system should be secure, because it mustn't enable duplicated votes and be absolutely clear, whereas protective the privacy of the attendees. The disadvantages of traditional voting system are that there is no reliability of voting. No assurance that people gave the votes is not changed before they are counted on the system. There is no transparency between the voter and the system. So, to overcome all these issues we are proposing to use block chain technology as a medium in the voting system. The purpose of such a scheme will be to provide a decentralized architecture to run and support a race plan, which is open, impeccable and independent verifiable. In this, we propose a potential the new e-voting protocol, which uses block chains as a transparent ballot box. Therefore, there would be more transparency between the user and the system. The advantages that we get while using the e-voting system would be to reduce election expenses including material, logistics and salary cost. People's opinion would be more public and more accessible by politicians and managers. If the voter is out of station, he can vote remotely. So, it strengthens the overall attendance. This paper we proposed blockchain based e-voting system in distributed peer to peer (P2P) network, system also proposed new mining as well as Conesus algorithm has proposed to achieve the higher accuracy. Some partial experimental analysis shows the how proposed system is better than traditional voting systems.*

Keywords: *Blockchain, Electronic Voting System, e-Voting, I-Voting.*

I. Introduction

Electronic selection machines are viewed as blemished, by the protection community, based totally on physical security issues. Anyone with physical access to such machine will sabotage the machine, thereby touching all votes run up the aforementioned machine. Enter blockchain technology. A blockchain could be a distributed, immutable, incontrovertible, public ledger. In each democracy, the protection of AN election could be a matter of national security. the pc security field has for a decade studied the chances of electronic selection systems, with the goal of minimizing the price of getting a national election, while fulfilling ANd increasing the protection conditions of an election. From the dawn of democratically electing candidates, the legal system has been supported pen and paper. commutation the standard pen and paper theme with a replacement election system is important to limit fraud and having the selection method traceable and verifiable our proposal modify participation of people or establishments within the following roles. wherever multiple establishments and people may be registered to identical role.

(i) Election administrators: Manage the lifecycle of associate election. Multiple trusty establishments and corporations square measure registered with this role. The election directors specify the election kind and build said election, configuration ballots, register voters, decide the period of the election and assign permission nodes.
(ii) Voters: For elections to that they're eligible for, voters will manifest themselves, load election ballots, solid their vote associated verify their vote when an election is over. Voters may be rewarded for choice with tokens once they solid their select associate election within the close to future, that might be integrated with a sensible town project.
(iii) District nodes: once the election directors produce associate election, every ballot sensible contracts, representing every choice district, square measure deployed onto the blockchain. once the ballot sensible contracts square measure created, every of the corresponding district nodes square measure given permission to act with their corresponding ballot sensible contract. once a private elector casts his vote from his corresponding sensible contract, the vote knowledge is verified by all of the corresponding district nodes and each vote they agree on square measure appended onto the blockchain once block time has been reached.
(iv) Boot nodes: every establishment, with permission access to the network, host a bootnode. A bootnode helps the district nodes to find one another and communicate. The bootnodes don't keep any state of the blockchain and is ran on a static information science in order that district nodes notice its peers quicker.

II. Literature Survey

Borge, Maria, et al. [1] Permission less blockchain-based crypto currencies generally use proof of work-of-work or proof-of-stake to ensure their security, e.g. to prevent double-spending attacks However, each approaches have disadvantages: prisoner results in huge amounts of wasted electricity and re-centralization, whereas major stakeholders in PoS could also be able to produce associate degree monopoly. during this work, we tend to propose proof-of-personhood (PoP), a mechanism that binds physical entities to virtual identities in a very manner that permits irresponsibleness whereas protective obscurity. Afterward, we tend to introduce PoP Coin, a replacement crypto currency, whose accord mechanism leverages PoP to eliminate the disadvantages of prisoner and PoS whereas ensuring security. PoP Coin leads to a continuously fair and democratic wealth creation process.

Bistarelli, Stefano, et. Al [2] Revive the Bitcoin e-payment system again and offer it as a decentralized end-to-end voting platform. Describe the main study choices behind the implementation, as well as pre-voting, balloting and post-polling steps. The ensuing implementation is totally decentralized: it's potential to vote directly in block-chain with none intermediate level. All votes are often verified by anyone reading the general public account of any individual. we have a tendency to conjointly use Digital plus Coins (through Open supply Assets) to trace votes, and we show election costs for n voters.

McCorry, Patrick, et al. [3] Using blockchains, introduce more and additional citizen privacy with the primary implementation of a suburbanized and self-matching web selection Protocol. Open Vote Network is appropriate for council chamber elections and has been written as a wise contract for thorium. not like the antecedently planned block-channel e-voting protocol, this is often the primary implementation that doesn't have faith in any reliable authority to calculate the Tally or shield the voter's privacy. Instead, the Open Vote Network could be a self-propelling protocol, and every citizen controls the privacy of its own vote, such it are often broken solely by collusion with all different voters. The execution of the protocol is enforced employing a accord mechanism that secures atherium block chains. we have a tendency to take a look ated the implementation on the official test network of Atheri to demonstrate its viability. In addition, we provide a financial and computational breakdown of its performance cost.

Khoury, David, et al [4] In a centralized environment, the results of voting events are always questioned and voted separately by the voters. Most existing e-voting systems are based on centralized servers, where voters should rely on organizing authority for the integrity of the results. In this letter, we propose a novel approach to a decentralized voting platform, which relies on Blockcon technology to solve the trust issues. The main features of this system are to ensure data integrity and transparency and to include a vote on every mobile phone number for every election, with assured confidentiality. To accomplish this, the Atherium Virtual Machine (EVM) is used as Blockline Runtime Environment, on which transparency, coherent and determinant Smart Contract will be deployed by the organizers for each voting program to run the rules of voting. . Without the need of third-party servers, users are certified through their mobile phone number. The results showed that the system is possible and one can move one step towards the ideal environment for such experience.

Lewis Tseng[5] Voting (or election) algorithms is widely used in many security-critical systems for mask errors. Most systems only tolerate malicious (or byzantian) voters - these systems recognize the existence of a right and centralized mechanism to collect votes and to disseminate each voter to the production of voting. However, in many realistic scenarios, such a centralized voting mechanism is not feasible. Thus, we study the Byzantine polling problem - no central mechanism exists in the system, and voters can become byzantine defective. We first offer impossible results in both synchronous and asynchronous systems. To circumvent the inconvenient results presented in two comforting voting properties, which are attainable and present optimal polling algorithms that satisfy comforting properties. Finally, we show that it is possible to design the Byzantine voting algorithm that produces polling production in a communication phase under dispute-free scenarios

Hardwick, Freya Sheer, Raja NaeemAkram, et.al [6] E-voting with Block Chain: An e-voting protocol with decentralization and voter privacy, which could be a potential answer to the shortage of interest in selection between young tech-savvy population. To become additional open, clear and freelance to e-voting, a possible answer would be supported blockchain technology. Blockchain explores the potency of technology and its quality within the e-voting theme. Associate in Nursing e-voting set up, that was then enforced. additionally to the challenges conferred by the Blockchain platform to develop complicated applications like e-voting, implementation and connected performance measurements area unit given within the paper. The paper exposes some deficiencies and presents 2 potential ways to boost the underlying platform (blockchain technology) to support e-voting and alternative similar applications. there's a great deal of promise in blockchain technology; inits current state, a system cannot reach its full potential. there's a desire to create a conjunct effort in core blockchain technology research for features and support for complex applications that can be executed within the blockchain network.

Navya A., Roopini R., SaiNiranjan A. S.et al. [7] System presented in The Electronic voting machine based on Blockchain technology and Aadhar validation that A nation with less voting percentages will struggle for development as the nation is very essential. Our proposed system is designed to provide secure data and a trustworthy election. Since this is the most important requirement for a personal identity, it is highly recommendable. Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. The proposed system is mainly designed for our country supported validation wherever the main points of the those that square measure higher than eighteen years square measure extracted from the bottom card info since it's become necessary within the gift situation. to make sure a lot of security, the fingerprint of citizen is employed because the main authentication resource. The system can permit you to vote through your fingerprint. As presently as they solid their vote, blockchain technology comes into existence, that is integrated within EVM By adopting Blockchain within the distribution of databases. This analysis discusses the recording of the voting result in blockchain algorithm from everywhere.

Dongsheng Zhang[8], Web traffic is extremely slim and unexpected. Load Balancer plays an important role in reducing uncertainty in web environments. Increasing adoption of cloud computing infrastructure, software load balancer has become more common in recent years. The current load balancer services distribute network requests based on the number of network connection of the backend server. However, when the other resources like CPU or memory backend servers are saturated, the load balancing algorithm cannot work. In the cloud computing environment, container-based software load balancer services used to evaluate and evaluate the flexibility and use. A plug-in framework that can dynamically adjust the weight assigned to each backend server based on real-time monitoring matrix.

Meter, Christian.[9]. System presents Design of distributed voting systems. The electronic voting system ideally tries to be easy to use and safe in the form of conventional elections and attempt to eliminate the described human errors. It is difficult to achieve, because the electronic voting system requires a strong encryption to guarantee the security, integrity and anonymity of the vote. It should be ensured and still as a result of a user friendly application, which is often difficult to obtain. But to assume that traditional elections are completely safe and correct to be true is also suspicious, because the system is already there, it is a good opportunity to think of computer and the use of cryptography to rein in the elections.

Gupta A, Patel J,et al. [10] System presented on the issue and effectiveness of Blockchon Technology on Digital Voting, Block Chain is a technology that enables the delivery of digital coins or assets from one person to another. The blockchain concept can be understood with the concept of linked list in the data structure, because its next key address is stored in the previous key and they are connected with each other. This was first conceptualized in 2008, which was implemented in the successive year as the main component of digital currency bitocaine, which acts as the public leader of all transactions. There are some issues and effectiveness in digital voting through blockchain technology, but our concern is to focus on how many systems make this technology more effective. Here, our main focus is on how the system can implement this technique in our daily lives. Our country India is deeply interested in the use of the future and a lot of efforts are being made to overcome the issues of security as soon as possible.

III. Proposed System Overview

IThis system highlights the implementation of e-voting using blockchain in distributed environment. The system consist two different phases like admin and user, initially user creates own profile with some inputs e.g. name, address, adhar No., PAN No. and other mandatory KYC details. Once user's registration has done, admin validate those users according to the desired policy. Valid user can do the voting to desire time, and concurrently system generates the each block in blockchian. During the execution system use SHA-256 for hash generation, mining algorithm for achieved the valid hash policy and consensus algorithm for validation all P2P nodes. This work aims to assess the request of blockchain as service to implement distributed electronic voting systems.

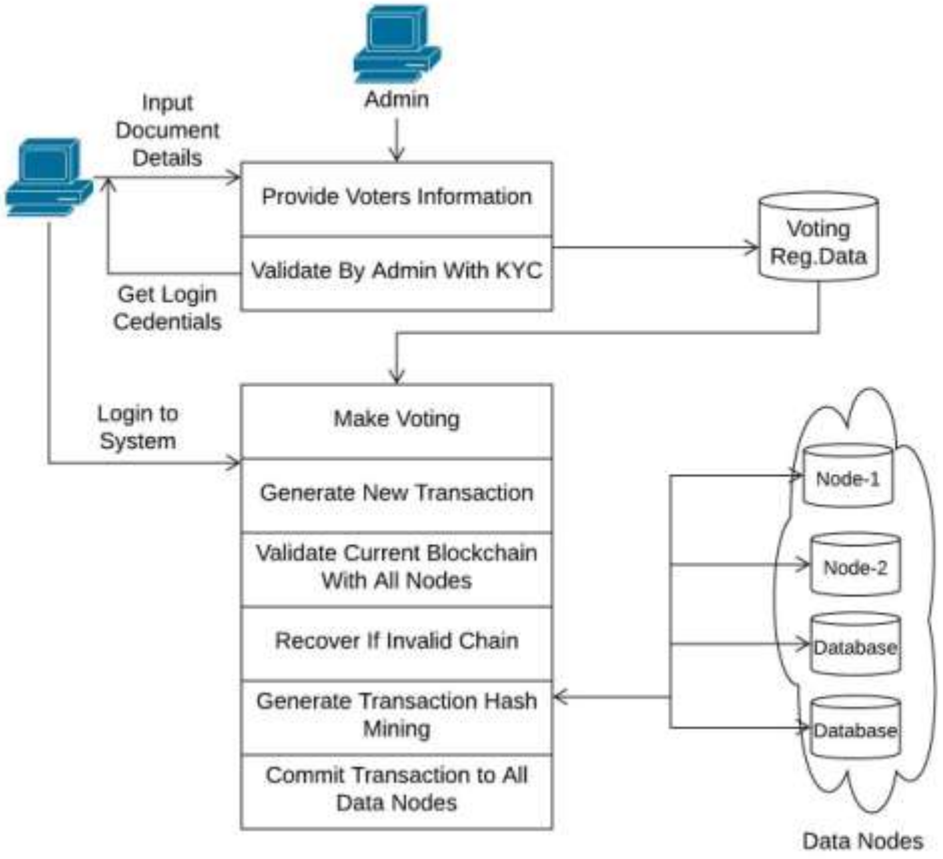

Figure 1: Proposed System Architecture

The main contributions of our add this paper area unit given as follows.

1. We tend to integrate the blockchain paradigm into e-voting procedure and are available up with a possible and general e-voting protocol while not a TTP, that provides a secure and versatile balloting mechanism, satisfies the majority of the most necessities for associate degree e-voting system and weakens the facility of the election organizer.

2. Consistent with the protocol, we tend to discuss many enhancements and extensions to satisfy the necessities of some specific situations.

IV. Algorithms Design

Algorithms 1: Algorithm 1: Hash Generation

Input: Genesis block, previous hash, data d,

Output: Generated hash H according to given data

Step 1: Input data as d

Step 2: Apply SHA 256 from SHA family

Step 3: CurrentHash= SHA256(d)

Step 4: RetrunCurrentHash

Algorithm 2: Protocol for Peer Verification

Input: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchainNodesChain[Nodeid] [chain],

Output: Recover if any chain is invalid else execute current query

Step 1: User generate the any transaction DDL, DML or DCL query

Step 2: Get current server blockchain

Cchain←Cnode[Chain]

Step 3: For each

```
$\text{NodesChain [Nodeid, Chain]} \sum_{i=1}^{n} \text{(GetChain)}$
    End for
Step 4: Foreach (read I into NodeChain)
            If (!.equalsNodeChain[i] with (Cchain))
                Flag 1
Else Continue Commit query
Step 5: if (Flag == 1)
          Count = SimilaryNodesBlockchian()
Step 6:Cacluate the majority of server
            Recover invalid blockchin from specific node
 Step 7: End if
            End for
            End for
```

Mining Algorithm for valid hash creation
Input: Hash Validation Policy P[], Current Hash Values hash_Val
Output: Valid hash

```
Step 1: System generate the hash_Val for ith transaction using Algorithm 1
Step 2: if (hash_Val.valid with P[])
            Valid hash
             Flag =1
Else
          Flag=0
Mine again randomly
Step 3: Return valid hash when flag=1
```

V. Results and Discussions

For the system performance evaluation, calculate the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.5 GHz i3 processor and 2 GB RAM virtual machine in Amazon EC2 environment. Table 1 shows the first experiment in our system. The below figure 2 total number of transactions and time required for execution of number of transactions.

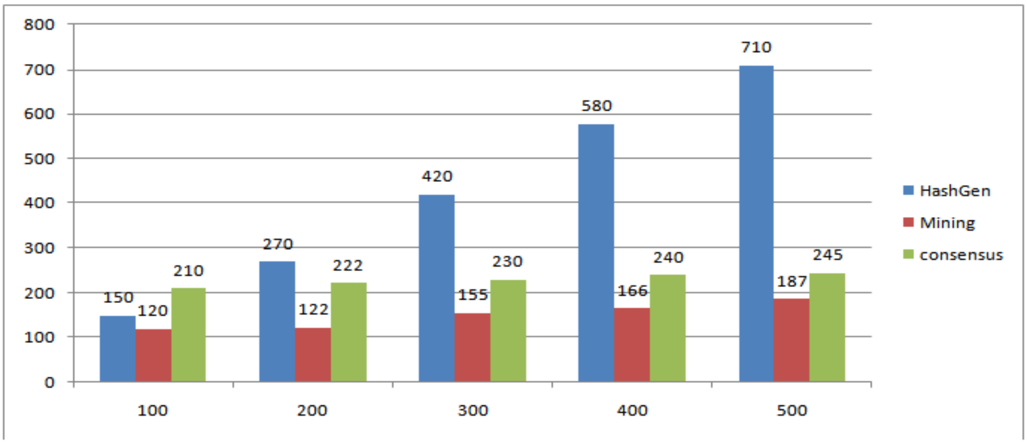

Figure 2: Experiment analysis base on different data size

The above figure 2 shows time required in milliseconds, the y axis shows number of milliseconds required for specific transaction size for hash generation, mining as well as consensus verification in P2P environment and x also shows the number of transaction for verification.

VI. Conclusion

In this paper, we tend to introduce a singular, blockchain-based electronic electoral system that utilizes good contracts to modify secure and price economical election whereas guaranteeing voters privacy. we've got made public the systems design, the design, and a security analysis of the system. By comparison to previous work, we've got shown that the blockchain technology offers a replacement chance for democratic countries to advance from the pen and paper election theme, to a lot of cost- and time-efficient election theme, whereas increasing the safety measures of the today's theme and supply new prospects of transparency. mistreatment associate Ethereum personal blockchain, it's potential to send many transactions per second onto the blockchain, utilizing each side of the good contract to ease the load on the blockchain. For countries of larger size, some measures should be taken to withhold larger turnout of transactions per second, for instance the parent & kid architecture that reduces the quantity of transactions hold on on the blockchain at a 1:100 magnitude relation while not compromising the networks security. Our election theme permits individual voters to vote at a pick district of their selecting whereas guaranteeing that every individual voters vote is counted from the proper district, that may probably increase elector turnout.

References

[1]. Borge, Maria, et al. "Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies." Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on.IEEE, 2017.

[2]. Bistarelli, Stefano, et al. "An end-to-end voting-system based on bitcoin." Proceedings of the Symposium on Applied Computing.ACM, 2017.

[3]. McCorry, Patrick, Siamak F. Shahandashti, and FengHao. "A smart contract for boardroom voting with maximum voter privacy."International Conference on Financial Cryptography and Data Security.Springer, Cham, 2017.

[4]. Khoury, David, et al. "Decentralized Voting Platform Based on EthereumBlockchain." 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET).IEEE, 2018.

[5]. Lewis Tseng." Voting in the Presence of Byzantine Faults".978-1-5090-5652-1/17 $31.00 © 2017 IEEE DOI 10.1109/PRDC.2017.11.

[6]. Hardwick, Freya Sheer, Raja NaeemAkram, and KonstantinosMarkantonakis. "E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy." arXiv preprint arXiv:1805.10258 (2018).

[7]. Navya A., Roopini R., SaiNiranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)

[8]. Dongsheng Zhang. Resilience enhancement of container-based cloud load balancing service. Technical report, PeerJ Preprints, 2018.

[9]. Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017).

[10]. Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1