



“Review on Decentralized E-Voting System Using Blockchain”

¹Sakshi Bachhav, ²Harshad Dhondge, ³Tejas Desale, ⁴Rohit Deshmukh, ⁵Prof.Poonam Deokar

[^{1, 2, 3, 4}] Student, ⁵ Professor

¹Department of Computer Engineering,

¹Dr D Y Patil College of Engineering and Innovation, Pune, India

Abstract: Voting process is right of every human being and this process is such complex and tedious process which involves lots of people in it. Previously voting can be done by using Paper-desk method and ballot method soon after age of internet introduced then EVM (Electronic Voting machine) comes in picture. But this EVM based voting has some security and the tampering related issue then EVM got banned in many countries like France, England, Iceland, later on Estonia comes with Internet based voting (E-Voting) but this method is vulnerable to cyber-attacks like DDoS attacks and Middle man attacks because it is based on the centralized system. Such problem needs to be tackled for making voting process secure and transparency then it observed that Blockchain Based voting can able to overcome the drawbacks which is present in EVM based voting system. Blockchain Technology is distributed public ledger which is in decentralized manner means Blockchain Technology does not need a central authority and it used hashing algorithm which make it nearly impossible to hack and immutable. E-voting using Blockchain Technology can overcome all the issues which are present in traditional voting process. Once the vote casted then it cannot be altered or tampered.

Keyword: Blockchain, Secure, E-voting, decentralized, Smart Contract

I. INTRODUCTION

Voting is said to be backbone of the democracy countries for their development by choosing right candidate can lead to great achievements hence elections are take places from very long time. The voting was carried out by using ballot method but that process is very time consuming and the duplication vote also take place [2].

The new age of internet comes and a new method of voting which is EVM (Electronic Voting Machine) are being used voting but tampering and security issue still the same and many countries even banned the EVM [4].

E-Voting is said to be more secure than the EVM but still it vulnerable to cyber-attacks. Such issues are the reason that people cannot trust the traditional voting process which ultimately suggest that we need another voting system which does not have the problems which are present in current voting system. When the Blockchain comes in existence it is found that using such technology in voting we can solve the problems which were present in the previous voting system.

The idea behind Blockchain Based e voting system arise when the Blockchain technology comes in existence. This Blockchain technology is distributed public ledger and has the characteristics of the decentralization, transparency and immutability [1].

Blockchain Technology is more secure than the centralized system and overcomes the security and tampering issues-voting based on Blockchain eliminates the used of the central authority and eliminate cyber-attacks involved in centralized system [3].

Smart contract is the business logic behind voting process, using web3 API and node.js provide good interfaces for the uses for better understanding of the process-voting based on Blockchain technology uses public key and private key. This is also used to authenticate the person is authorized or not. The idea behind the E-voting is similar to the digital wallets [4]. Once the vote is casted only public key will be visible to all and identity of the voter remains unknown to everyone. Blockchain is chain of blocks and this blocks stores the vote and connected to the other block and protected by the hashing algorithm even if someone has access to the terminal he cannot tampered the vote after it has been casted.

II. SYSTEM MODELS

i. Blockchain Technology

The idea of the Blockchain technology is discovered by the scientist Stuart Haber and the W.Scott using cryptography secure chain concept to store the document. Later on in 2008, Satoshi Nakamoto public paper based on cryptocurrency known as Bitcoin and give concept of distributed Blockchain. The study of Blockchain was steady and has scope in Finance and trading sector later on in 2013 Vitalik Butrin introduced Ethereum which has smart contract technology and now Blockchain technology can be used in other sector rather than finance or trading

ii. Smart Contract

Smart contract the business logic (code or programmed) used in the Blockchain technology. This smart contract and executed when the precondition met and once they get deployed it cannot be modified [1].The feature of smart contact was developed in Blockchain 2.0.This smart contract are written using language

iii. Web 3.0

Web 3.0 is the iteration of the World Wide Web and it is decentralized technology. Web3.0 runs on the Blockchain technology and this is trustless and permissionless system introduced by Gavin wood along with the Ethereum Blockchain.

III. REVIEW ON BLOCKCHAIN VOTING

There are many practices are made to introduce many variations in electronic and online voting system which are used many techniques and methodologies. Where some are gives promises about confidentiality and integrity to system but after research and testing, they have many vulnerabilities. Important purpose of voting system is to privacy of voters and their voting information. Also it is also required to emphasize on Advanced system is find for Managing and controlling the whole voting system. Many system which guarantees secured electronic and online voting system their basic approach is taking votes with the help of electronic devices and online portals [2].

It provides security to voting data with the help of different encryption and decryption techniques. In this previous voting models and architecture they operate on centralized system approach. And centralized system sometimes have security issues. Just like because of when we collect data in centralized system we take a risk about data storing and security [9]. Also it can be controlled unfairly. So for overcoming this problem we take help of Blockchain. Blockchain is distributed ledger that stores all processed transaction in chronological order. Also the traditional databases are maintained by a centralized or single organization, they also have to control all over database and also they able to do changes unfairly in database [1].

They have complete control on it.They also have the ability to manipulate with the stored data, to censor otherwise valid changes to the data, or to add data fraudulently. For most use cases, this is not a problem since the organization which maintains the database does so for its own benefit, and therefore has no motive to justify whether unethical practices in database's contents. There are other use cases, such as a financial network, where the data being stored is too sensitive and the motive to manipulate it is too enticing to allow any single organization to have total control over the database [4]. Even if it could be guaranteed that the responsible organization would never enact a fraudulent change to the database there is still the possibility that a hacker could break in and manipulate the database to their own ends.

Blockchain Technology solves this problem by Creating a network of nodes of means network of computers. Each node is stored a database copy. Also they have a set of rules. Which define the order in which nodes may take turns adding new changes to the database. In this way, all of the nodes agree as to the state of the database at any time, and no one node has the power to change the data .Hence the integrity of database is get maintained by it.This special characteristics gives us powerful database with security. The Blockchain further requires that an audit trail of all changes to the database is preserved, which allows anyone to audit that the database is correct at any time [5]. This audit trail is composed to the individual changes to the database, which are called transactions.

A group of transactions which were all added by a single node on its turn is called a block. Each block contains a reference to the block which preceded it, which establishes an ordering of the blocks. Hence because of it also called as Blockchain [1]. Blocks hold batches of valid transactions that are hashed and encoded into hash value and each block includes the cryptographic hash of the prior block in the Blockchain, linking the two. The linked blocks form a chain. A Blockchain establishes the order in which transactions were applied to the database so that anyone can verify that the database is accurate by rebuilding it from scratch and verifying that at no point was any improper change made.

comparison between traditional voting and blockchain based voting.

Traditional Voting	Blockchain Based Voting
EVM(electronic voting machine) are been used	Blockchain Interface with Ethereum Virtual machine and smart contract will be used.
Need a Central authority to take decision and control on everything	No central authority will required, it will publicly distributed ledger
Vote can be tampered	Vote will not be tampered
Security is less	Security will be more
Confidentiality and Integrity of vote get compromised	Confidentiality and Integrity of Vote surely will be maintain

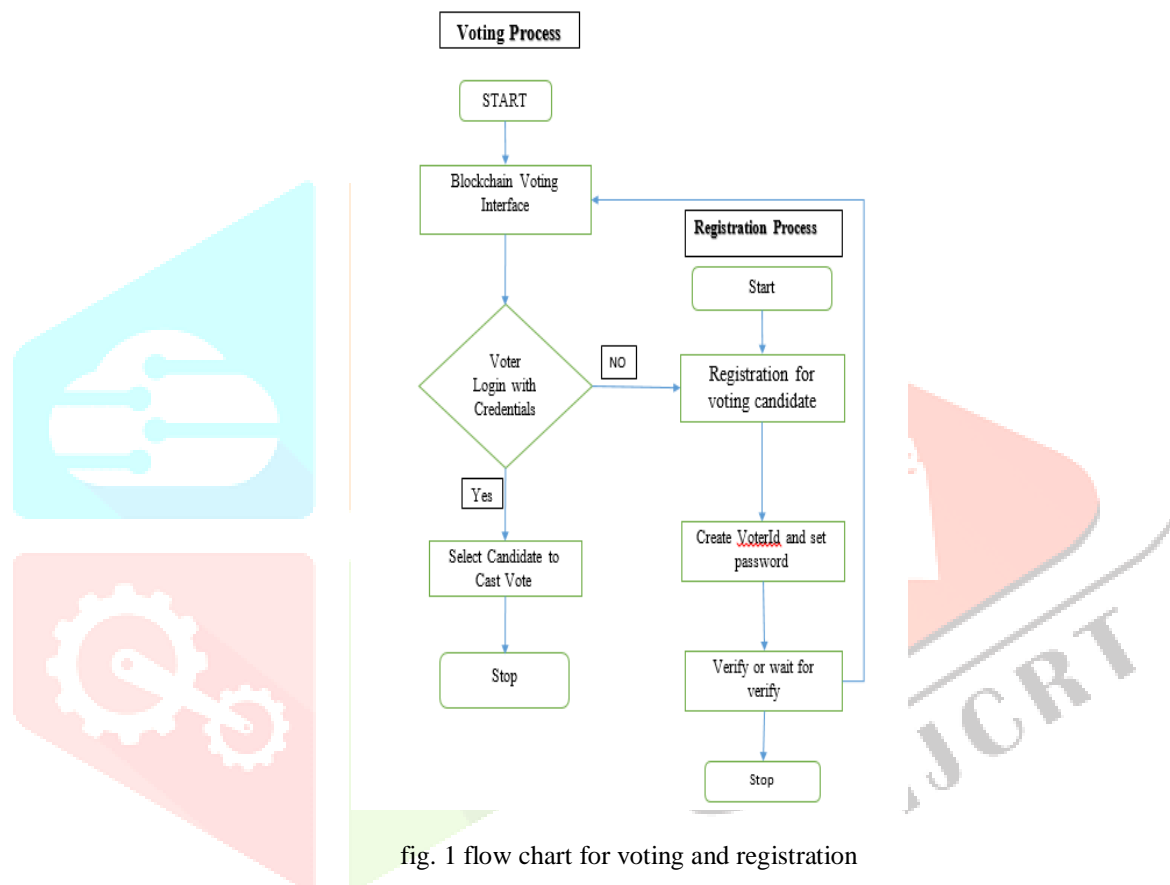


fig. 1 flow chart for voting and registration

IV. CHALLENGES IN SYSTEM

a. Scalability:

Blockchain Technology is complex to design, if large peoples get involved the scalability issue will be rise. It is hard to scale the Blockchain network result is that Blockchain Network becomes dull for the users.

b. Skill Person are Required :

Blockchain is complex in nature and required validators and the miners to run blockchian network without any interruption from the external sources hence skilful person are needed to maintain Blockchain network to run without any failure.

c. Speed of internet:

Blockchain network need high speed internet connection to run without any interruption. In many region the access for high speed internet connection in not evolve to that extent which is needed for the blockchian so It may be hindrance our proposed system.

V. CONCLUSION

Our proposed E-voting based on Blockchain provided more security and transparency than existing voting process. Smart contract are immutable code or programmed are used to add functionality in voting process and web3 libraries provide great Blockchain based framework for performing e-voting. The Vote Cast by the voter permanently stored and never be tampered by anyone and the identity of the voter will not be disclose to anyone. Smart contract with Blockchain network protects the anonymity and the confidentiality of the votes. This E-voting based on Blockchain is the voting process on which people and rely on and trust that vote is casted to right person and never been tampered.

VI. REFERENCE

- [1] Y. Zhang, Y. Li, L. Fang, P. Chen, and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchain and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications, doi: 10.1109/iccc47050.2019.9064387
- [2] P. Raghava , P. Uday Kiran, Vimali. J. S, "Trustworthy Electronic Voting using Adjusted Blockchain Technology,"2020, ISSN Conference 2321 3361 © 2020 IJESC.
- [3] Rajat Gupta ,Bipul Jha,Atul Kumar Shukla,Aryan Raj and Dr Shabana Sultana."Secure and Decentralized Smart Elections,"IOSR Journal of Computer engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727(Jul-Aug 2020)
- [4] Kriti Patidar, Dr. Swapnil Jain, " Decentralized E-Voting Portal Using Blockchain", 10th ICCCNT Conference 2019, DOI: 10.1109/ICCCNT45670.2019.8944820
- [5] Aaron Fernandes, Karan Garg, Ankit Agrawal, Ashutosh Bhatia, "Decentralized Online Voting using Blockchain and Secret Contracts," 2021 International Conference on Information Networking (ICOIN) | 978-1-7281-9101-0/20/\$31.00 ©2021 IEEE, DOI: 10.1109/ICOIN50884.2021.9333966
- [6] Kanika Garg, Pavi Saraswat ,Sachin Bisht, Sahil Kr. Aggarwal ,Sai Krishna Kothuri ,Sahil Gupta,' "A Comparative Analysis on E-Voting System Using Blockchain , "2021 International Conference on Information Networking (ICOIN) 978-1-7281-1253-4/19/\$31.00 © 2019 IEEE,DOI: 10.1109/IoT-SIU.2019.8777471
- [7] Ali Mansour Al-madani, d Dr.Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T.Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology, "International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, DOI: 10.1109/ICSIDEMPC49020.2020.9299581\
- [8] Ashish Singh Kakali Chatterjee "SecEVS : Secure Electronic Voting System Using Blockchain Technology," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), DOI: 978-1-5386-4491-1/18

