IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 13, Issue 3, March 2023, ||Series -I|| PP 17-21

Block chain Based Decentralized Voting System

Ritik Paliwal[1], Vishal Chavan[2], Harsh Sonwane[3], Vikas Rathod[4], Prof Shailesh Gawai[5]

JSPM's RajarshiShahu College of Engineering, Tathawade, Pune-411033 Department Of Information Technology

Received 10 March 2023; Accepted 23 March 2023

Abstract.
Nowadays cryptocurrency has become a trending topic in the software world. Blockchain is the backbone of Cryptocurrency. The objective of this project/survey is to use blockchain technology in voting systems. Blockchain is a decentralized technology. Blockchain stores transaction information that can be used to review the trustworthiness of transactions. Blockchain is a digital ledger of economic transactions that can be programmed to record financial as well as other transactions, it is difficult to forge. The required transaction for running code is properly written in the solidity programming language created by the Ethereum system and can be run on the remix IDE of the Ethereum blockchain system. We need gas for each transaction and it will be deducted from our Metamask wallet created by us. Metamask wallet is a type of digital wallet for digital currencies. Since the information stored in the blockchain is not associated with personally identifiable information, it has at-tributes of anonymity. Blockchain allows transparent transactions and verification. These blockchain technologies' characteristics are helpful in a voting system that is strong, robust, and transparent. The Voting System is the heart of our country.

Keywords.
Blockchain, Smart Contacts, Solidity, Ethereum, Web3, Voting, EVM (Ethereum Virtual Machine)

I. Introduction

We proposed a method in which valid people can vote from their mobile phones themselves from any location. The main purpose is to make elections transparent and decentralized using blockchain technology based on the Ethereum Virtual Machine(EVM). They don't need to go to the voting center and wait in a queue for a certain period of time. By verifying and registering themselves on the decentralized voting app they can vote from the mobile devices having digital wallets. The blockchain was popularized by a person/group of people using the name Satoshi Nakamoto in 2008. A blockchain is a collection of data, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published to get into the corresponding hash. As blocks, each contains information about the block previous to it and then they form a chain, with each additional block one before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered without altering all subsequent blocks**.**

II. LITERATURE SURVEY

2.1] A Research Paper on Blockchain-based E-Voting System

Authors: Authors: Adarsh.G.Vernekar, Mahesh Phutane, Rohit Godse, Vinayak Waghmode, Mr.S.M.Shinde

The present election system doesn't supply transparency in tally votes. There square measure many threats in the current legal system like pretend voters, malpractices on
polling booths etc. Blockchain's primarily-based electronic voting system will overcome all the problems that square measure within the current election systems. Blockchain technology will give multiple properties thanks to its distributed ledger technology. Blockchain may be a decentralized machine and knowledge sharing platform that permits multiple authorities who do not have trust among them; however , they join forces and collaborate in deciding procedures. Blockchain may be a chain of interconnected blocks that has all the knowledge of the user through distributed ledger technology. In our blockchain primarily based election system we've outlined Associate in Nursing election as a wise contract. Therefore in our network election is considered as Associate in Nursing agreement between the taking part nodes.The good contracts square measure defined consequently with relation to roles outlined to the participants inside the network. The election method consists of multiple procedures to be disbursed in it.[1]

2.2] A Research Paper on Prevention Of Voter Fraud Using Blockchain Technology
Authors: NishkarshBareja, K.Swapnil

Voter Fraud without a doubt has been catastrophic at so many levels. The wrong leader makes wrong decisions which starts a domino effect of bad decisions thereby affecting the nation. Our constitution gives us the right to vote and voting is a very crucial aspect of the progression of a country. It is the most basic civil right on which all other rights of the people may depend. When selecting a municipality counselor or even the Prime Minister of a country, every constituent should be able to trust the procedure and outcomes, or it would be a loss of democracy. Any meddling with the votes or the election results is considered voter fraud. Frauds also include buying votes, violence against the constituents, mix recording of votes, destruction of ballots, and tampering with electronic voting machines.[2]

2.3] A Research Paper on E-Voting Using Blockchain Technology
Authors: Tanikella Sai Charan1, SrinandaPentapati, Mrs. R. Prema

An electronic voting system that uses blockchain technology completes the stage of establishing a secure and transparent environment for decisions where voters will actually want to vote only once and the vote will not be interrupted. The operation of the blockchain will ensure that the votes are kept in line with them and that the situation is not deceived by any outsider. Protected electronic voting structures use a blockchain which is a separate, distributed, and tracking transaction record that follows peer-to-peer transactions. Each vote given will be considered a role as one job. These votes will be counted and the results will be reported immediately. Voting is a very important and important event organized in all countries by secret ballot or by ballot. Such processes have many drawbacks such as vote disruption, low turnout, and so on. To overcome all this, we will introduce a series of voting programs.[3]

2.4]A Research Paper on Blockchain-based E-Voting System
Authors:Pallavishejwal , Aditya Gaikwad, Nikhil Jadhav, Mayur Anawar, NoorMohommadShikalgar

A nation with a low turnout will struggle to develop because it is imperative for the nation to choose the right leader. A system designed to provide secure data and reliable e-voting among the people in our proposed democracy. The blockchain itself is used in a bitcoin system

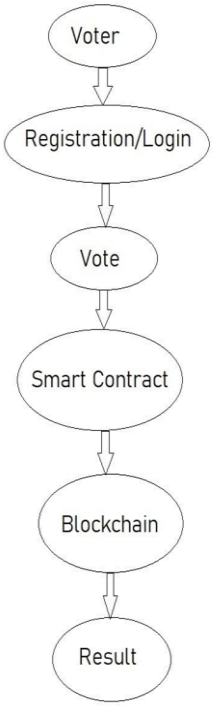


Fig.1 Voting System Overview

3. Proposed System
In Proposed system we have introduced some new features and new methods so that the proposed system can stand out differently from other surveyed systems

3.1 Registration :
In this step there will be the registration process in which each voter has to register first by filling in required details like, name, metamask id, Email address, identity, age etc. along with that voter has to provide some documents for verification. Through an Application interface connected with blockchain via smart contracts written in solidity.

(1) Every voter is issued a credential by the voting office / Blockchain provider in a secure way, which includes a unique identity ID and a list of candidates registered.

(2) Every voter gets a generated private key randomly from server/blockchain.

(3) Every voter computes the public key based on the private key.

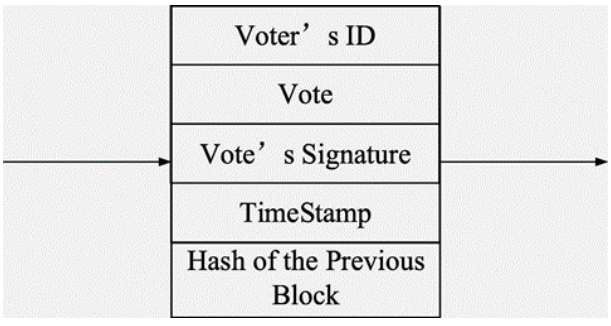
(4) Voters keep their private keys

3.2 Login :
In this step there will be to login through the mobile voting application. After entering the public key and private key the hash value or signature will be generated and another hash value is generated by miners if both match then only the user will be able to login successfully and proceed further for the voting process.

3.3 Voting :
(1) Voter will vote using its id and password

(2) This vote will be sent through the smart contract to the miners and then to the blockchain
.(3) The miner uses the public key to verify entered details′.
(4) The miner queries and verifies that the voter has the right to vote or enough votes.
(5) The miner generates a new block with the previous block's hash value and the information of vote and adds it to the blockchain.
3.4 Security :
(1) Anonymous: each user in a blockchain-based e-voting system uses an ID instead of his real identity and the system is decentralized without a third party. Thus, the privacy of the users is protected.

(2)Hashing Algorithms : Best hashing algorithms are used in this system which will protect the system from any attacks.



3.5 Result of Voting :
(1) Votes are updated after each vote is done.

(2) The functions of smart contracts are written in the solidity language will do this results update work.

(3) At last Voting results are available on the app itself only.

4.1 Architecture

(1) Voter uses Eth-Hash(SHA-256) to generate the hash value of H=Hash(ID + Vote + Timestamp).
(2) Voter uses his/her private key to generate a signature S of the hash value H.
(3) Voter sends ID(Metamask ID), Vote, Timestamp, S to the miner.
(4) The miner obtains the public key from the server according to voter's ID.
(5) The miner uses Eth-Hash(SHA-256) to generate the hash value of H=Hash(ID+Vote+Timestamp).
(6) The miner uses the public key to verify S and get H′.
(7) The miner compares H and H′. If H and H′ are the same, S is accepted. Otherwise, it is rejected.
(8) The miner queries and verifies that the voter has the right to vote or enough votes.
(9) The miner generates a new block with the previous block's hash value and the information of vote and adds it to the blockchain.
Besides, the voter can withdraw his/her vote before a preset deadline. The withdrawal process is similar to the voting process.

Fig.2 Blockchain Properties

4.2 Algorithms :
Hashing Algorithms : Best hashing algorithms are used in this system which will protect the system from any attacks.
Eth-Hash or **Keccak-256** is a new hashing algorithm created by Ethereum itself; it is another form of SHA-256.

5. Future Scope
○Blockchain is the future itself.
○Easier, cheaper, faster, secured, and transparent voting environment.
○Blockchain-based Electronic Voting system is a boon to the modern society of a nation.
○ No need to stand in a long queue to vote.
○ Voting is possible from anywhere.

6. Conclusions
In this work, we introduced a Blockchain-based secure E-voting system that enables the decentralized database to cast votes in a modern way. We have shown that blockchain technology can solve the security, transparency, fairness, and trust issues and it is offering to reduce the barriers of E-voting systems. Blockchain technology will be openly verifiable and distributed so that nobody will be capable of corrupting it. We also presented the drawbacks of our E-voting system, which will be adopted in the upcoming study.
● The primary motive for initiating the decentralized electronic voting system is to make the election process cheaper, secure, faster, easier, and more transparent for society.
●During this paper we've focused on the Ethereum blockchain-based voting system that guarantees cost efficiency, privacy, and security to the election procedure.
●We've also focused on the security issues within the E-voting system. This election system will provide a verification to voters and transparency is maintained throughout the system about his casted vote.

Reference:

[1]. A Research Paper on Blockchain-based E-Voting Systems. .(IRJET)-International Research Journal of Engineering and Technology. Authors: Adarsh.G.Vernekar, Mahesh Phutane, Rohit Godse, Vinayak Waghmode, Mr.S.M.Shinde. ISO 9001:2008
[2]. A Research Paper On Prevention Of Voter Fraud Using Blockchain Technology.(IRJET)-International Research Journal of Engineering and Technology. Authors: NishkarshBareja, K.Swapnil. ISO 9001:2008

[3]. A Research Paper on E-Voting Using Blockchain Technology.(IRJET)-International Research Journal of Engineering and Technology. Authors: Tanikella Sai Charan1, SrinandaPentapati, Mrs. R. Prema. ISO 9001:2008

[4]. A Research Paper on Blockchain-based E-Voting System. .(IRJET)-International Research Journal of Engineering and Technology. Authors: Pallavi shejwal , Aditya Gaikwad, Nikhil Jadhav, Mayur Anawar, NoorMohommadShikalgar. ISO 9001:2008

Ritik Paliwal, et. al. "Block chain Based Decentralized Voting System." *IOSR Journal of Engineering (IOSRJEN)*, 13(3), 2023, pp. 17-21.