Decentralized E-Voting System Based On Blockchain

LEELA JANCY P
ASSISTANT PROFESSOR, Department of IT,
SRI SAIRAM INSTITUTE OF TECHNOLOGY
Chennai, India

PONMALAR.A
ASSISTANT PROFESSOR, Department of IT ,
,SRI SAIRAM INSTITUTE OF TECHNOLOGY
Chennai, India

Abstract* — Voting is a major factor to change the country's future. Elections in India are challenging ones with more than 800 million voters and nearly 2,000 political parties involving. difing the result of the final result, stealing the Electronic voting machine and election manipulation are the major issues in the current voting system. In 2017, it was found that eighteen electronics voting machines were registering votes for the wrong party in Rajasthan. As like this ,more no of cases are there in the country.To overcome these issues we suggest a decentralized system to be integrated with the voting system. Oneofthosedecentralizedsystemsisblockchain.Tocreate an electronic voting systems in a distributed manner, this model evaluate the application of block chain .Theproposed systemhasamoreprominentsecurityaslikehighsecurity voter secretwordisconfirmedbeforethevoteisacknowledgedinthe database of Election Commission of India.Using block chain technique we can improve security as well as it helps to implement online voting system without any malicioususer.

Keywords* — *Decentralized ,Electronic voting , Blockchain .

1. INTRODUCTION

In a democracy, government is chosen by conducting election through voting and speaking clearly, national security is measured by voting system also. Election security is to protect voting structure from issues like cyber attack or cyber threat like voting machines and equipment infiltration,election office networks and voter registration databases. Voting fraud is neither present nor absent everywhere. In our country, there have always been allegation of fraud by all the losing political parties. A voting system which was created malicious and distributed to thousands of polling booths, can systematically falsify billions ofvotes. For ensuring the election integrity, we are using blockchain. Blockchain is a decentralized, immutable, public ledger. IT is a distributed ledger which can record transactions between two parties in a verifiable manner. Blockchain uses cryptography that links growing list of blocks.

The three main features of blockchain are:

*[1] **Immutability**:*

In the blockchain data cannot be altered. Each block holds a cryptographic hash of the previous block.Once recorded the data in any block cannot be changed without alteration of subsequent blocks.This creates immutable chain and maintains the integrity of the blocks.

*[2] **Decentralizedconsensus**:*

Decentralization is the process of distributingpower away from the central authority. A decentralized consensus protocol determine who can add the next new transaction to the ledger. All blocks must reach a consensus before any new block enters as a permanent part of theledger.

*[3] **Verifiability:***

The blocks are distributed over different locations. This provides third party verifiability as all the blocks maintain the consensus version of the ledger.

Blockchain security methods use public key cryptography as an address on the blockchain.A private key gives access to the digitalassets like a password.

This system proposes the use of blockchain to implement an electronic voting system and its goal is to provide security along with cost reduction in conducting an election.

Such mistrusts creates are multiple disadvantages and they create national problems like:

- *Instability in Political*
- *Compromised writ of thegovernment*
- *Mistrust over the electoralprocess*
- *Compromised governance*
- *Disorder in the stateinstitution*
- *Chain of command to run stateaffairs*

S.No	***Reasons***	***Description***
1	*Pre-poll rigging*	*This includes but not limited to the (sometimes intentional) errors in the voting lists and formation of the voting districts to help one and hinder other parties. In some areas the polling stations are made too far that the voters prefer not to vote than going too far tovote.*
2	*Casting duplicate votes*	*Since there is no biometric authentication on the polling stations , it is easy to cast vote again for the ones who have not voted . Sometimes there are thousands of ballot papers found voted without presence of actualvoters.*

3	*Use of power to influence polling staff*	*The use of power is not uncommon to influence the voters either by incentives or by threats.*
4	*Unsupervised vote counting*	*For parties or independent condiments who do not have a strong representation in a region, it is likely that their votes can be miscounted.*
5	*Lack of audit andappeals*	*The process of hearing and deciding appeals on such issues is so slow that they can hardly be finalized before the next elections. Therefore, the losing candidates and/or the losing parties start the street agitation instead of going to the constitutional bodies to get the conflicts resolved. This causes in unrest and political instability in the country.*
6	*Lack of interest by public at large*	*By observing the reasons in 1-5, there has been a feeling that the people are not fully convinced to vote and the mistrust on the voting system has taken over their right of participation. Such issuescan be dealt with the trustworthy electronic voting platforms.*

2. RESEARCH BACKGROUND

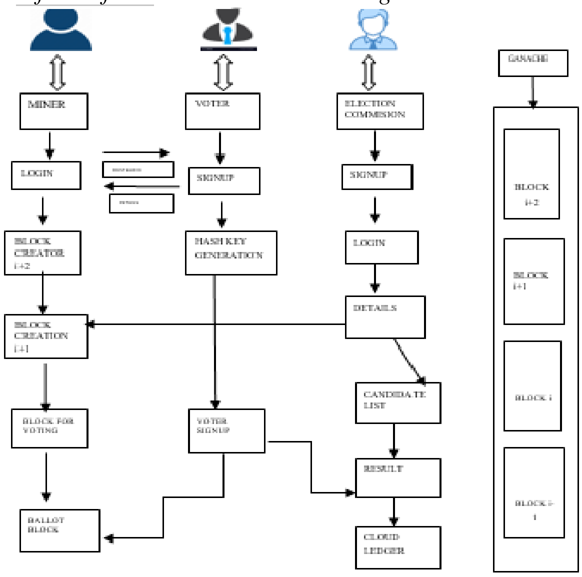
Even in the developed countries,mistrust in the voting is not a uncommon event .Few countries like e.g. Germany, Belgium and Norway used the e-voting systems in the past while some countries dropped it due to audit problems. Even having an e-voting system,Switzerland still allows the voters to cast their votes either by mail or by casting the vote in the polling stationindividually.For a voting system to become completely dependable ,the e-voting system requires more integrity,more security, more privacy, and more transparency. Basin et al. [3] has presented an example from the canton of Valais Switzerland in March 2017, where the voters not received the postal ballots and when they were re-issued, it was noticed that right of the citizen had already been casted. Rivest [5] has presented the concept of providing the voter with three ballots where the voter have to cast all the ballot papers after marking. Due to th decrypted key,everyballot paper includes a unique identification number but the voter remains unknown . At the time of tabulation, the casted votes are linked and the choice found on two ballot papers is chosen while the other ballot paper's choice is rejected. The scheme may not be used effectively in situations like there exist only two contestants or if there exist more number of contestants. The disadvantage of the scheme like being slow and the human error increase if the votes are not accurately polled in the respective boxes. The private or the collective blockchain which is maintained by an organization, e.g.election commission of the country, need a resolution strategy in place. In the private blockchain only the eligible nodes can see the details of the votes and the transaction.The voting process remain non visible to the voters. This makes the voting process less transparent than paper based voting. The electronic voting system is expected to have a great glorious future . In some countries e-voting is not an option while few countries are in the process to eliminate thesecurity, verifiability, and anonymity concerns.

3. METHODOLOGY

3.1. ARCHITECTURE

The voting scheme that uses block chain is public, distributed, and decentralized.Votesfrom voters across many mobile devices and computers can also be recorded. The network cannot be influenced by a single party because of its decentralized property. To avoid forgery during voting ,this system provides a synchronized model of voting records based ondistributed ledger. The blockchain based voting scheme allows the voters to audit likewise to verify the votes. Thevote database is managed autonomously. This model opens up many possibilities to secure the voting system and help for the welfare of thenations.

Fig 1: Architecture Diagram



3.1.1 Attaching the polled vote to thecorresponding block in Blockchain:

Once a block is created, the information regarding the voter and voting process is recorded in the block in block chain . Each block is linked to the previous block .

3.2 MODULES:

3.2.1.Checking the authentication of voter:

The user must login to the system using their credentials based on details like name,address along with the number that confirms that the voter has casted his/her vote is e

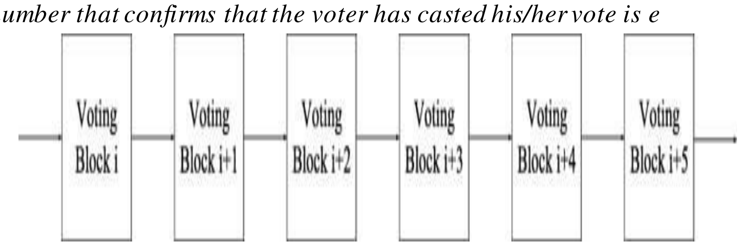


Fig 2: Creation of Block

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 03 | March - 2021 *ISSN: 2582-3930*

provided to registered voters by the authorities, the e-voting system will compare those details entered by the user and those details with them. All the information entered by the user will be checked by the system and, if it matches a legitimate voter, the user will beconsidered as correct voter and he/she will be eligible to cast their vote .

3.2.2.To cast the vote:

Voters can choose from either to cast a protest vote or to vote for one of the candidates. Vote casting will be done through interface that is user friendly .A token(also referredasEthereum)is generated for each voterwith aninitialBooleanvalue as one.once the voter cast his/her vote, the Boolean value becomes zero. A voter can cast a vote if and if only the Ethereum value is 1. In this way re-voting problem can also be resolved.

3.2.3. Votes are Encrypted:

Once the citizen poll their vote , the system will automatically produce an input that includes details like unique identity number ,voter's name and previous polled vote's hash code. The input and the encrypted output are unique.As soon as the vote is polled ,each vote will be encrypted and header of the block store the encrypted value.so both encryption and hash function are being used to enhance both privacy and authentication.Each Voter's details are encrypted using irreversible one way hash function SHA . The only possible way to reverse the hash would be to guess the original data and the encryption method and then hash it to see the results are match. This way of hashing votes makes it nearly impossible to reverse; thereforeit is impossible to retrieve the voter'sinformation.

3.3BLOCK CREATION:

The needed one is to create blocks before the occurrence of transaction .The transaction takes place in the concerned blocks. The voting office verifies both the identification number of the corresponding voter and their authentication related to biometric one. Next the hash code is generated by the system using SHA algorithm so as to provides authentication. In the block header,the hash value of each block is computed and saved for validation purpose.The hash value is obtained by finding the hash algorithm SHA-521 which is very effective in providing authorization.Depending upon on the hash value of the first block, the authority office will provide the identity number for the nextblock creation.

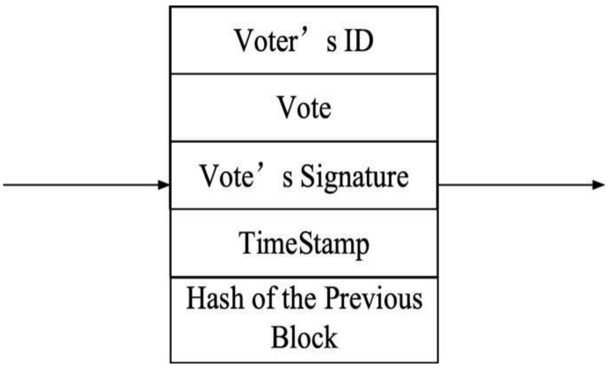


Fig 3: Vote Block

Potential threats to security and privacy which can overcome by blockchain . Nanotechnology increase the electronics devices capabilities while we reducing their weight and power consumption. This technology improves the efficiency and working of electronic voting and binding with the technology of block chain.

5.SYSTEMDESIGN:

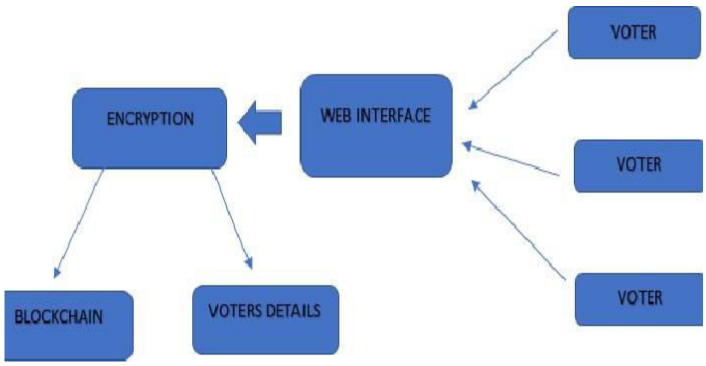


Fig 4: System design

5.1.PROPOSEDSYSTEM:

The first transaction of the block is a transaction that will be considered as the candidateone.During this transaction, a block will be created and it contains informations like candidate name and this is going to be the main block and the candidate's vote is placed over the main block. The main block is not taken as vote, and it includes the name of the candidates. Our decentralized e-Voting system will also allow a protest vote, where the voter can return a blank vote to notify lack of satisfaction with all the candidates or a refusal of the current political system and/or election. Every time a person votes the transaction will be recorded and the blockchain will be updated.

To improve the safety of the model ,thecurrent node/block will include the information of previous voter. If any of the blocks were altered, then it will easily indicate the malpractice since all blocks are connected to each other. The model is not centralized and cannot be corrupted, no single point of failure exists. Once the vote sent to one node in the system ,the node adds the vote to the blockchain. The electoral system will have a node in each district to ensure that the system is decentralized.

6..LIMITATION

Few assumptions that are accepted in this paper-

1.The voter don't know about the voting process. It is important that each voter can vote in their specifiedtime.
2.The information is to be obtained from any agency in line with the election commission that maintains the data forthe verification purpose.It is also assumed there exists uninterrupted network connectivity available all the time,communication can be carried out with out delay and there exists uninterrupted internet connectivity.

3.Assumed that the technology aware supporting staff should be there and they should assist the citizensto poll their vote .

7.CONCLUSION

We have introduced a electronic voting system based on blockchain employing smart contracts to provide secure and cost-efficient election while assuring the privacy of voter. In this paper, we have noted that the blockchain technology offers a new possibility to defeat the challenges and limitations of electronic voting systems which ensures the election security and lays the ground for transparency. Block chainapplications have to be formally verified. Misusing a smart contract for material replenishment will make a lot of impairments in the supply chain. Recent hacks have shown that attacks on the overall Block chain application will be dangerous and costly. Therefore, it is necessary to include techniques that verifies Block chain applications for supply chains.Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain by running every prospect of the smart contract to simplify the load on the blockchain. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system. It is summarized that registering the Voters details in the cloud with block chain improves efficiency and also avoid malicious users.

REFERENCES

[1] B. Shahzad; J. Crowcroft , "Trustworthy Electronic Voting Using Adjusted Blockchain Technology" , 2169-3536/25 ©2019 IEEE

[2] Emre Yavuz ; Ali Kaan Koç ; Umut Can Çabuk ; GökhanDalkılıç , "Towards secure e-voting using ethereum blockchain",2018 Sixth International Symposium on Digital Forensic and Security(ISDFS)

[3] D.Basin,H.Gersbach,A.Mamageishvili,L.Schmid,and O. Tejada ,``Election security and economics: It's all about eve,'' in Proc. Int.JointConf.Electron.Voting,2017,pp.1_28.

[4] HaijunPan ; Edwin Hou ; Nirwan Ansari , " Ensuring voters and candidates' confidentiality in E-voting systems" , 978-1-61284-680-4/11/$26.00 ©2011IEEE

[5] R. L. Rivest, ``The three ballot voting system,'' Tech. Rep., 2006, p. 15

[6] Shalini Shukla ; A.N. Thasmiya ; D.O. Shashank ; H.R. Mamatha ," Online Voting Application Using Ethereum Blockchain" , 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 978-1-5386-5314-2/19-20 ©2018