Blockchain Based Decentralized Voting System

Shrey Garg, Deepak Kumar, Saroj Kumar Manna, Simran Chauhan, Dr. Rani Astya
School of Engineering and Technology
Sharda University
Knowledge Park III, Greater Noida,
Uttar Pradesh - 201310

Abstract- It's always been a challenge to create a new voting system keeping in mind at the same time,of the legal factors that are associated with it. The old systems, the old computer technology has been proven vulnerable to threats and hence the need for new technology has risen exponentially. Block chain as a technology has many benefits over its existing methods. And hence we are aiming to test these features of blockchain in our electronic voting system. We propose a new block chain-based decentralized electronic voting system which deals with all the discrepancies, all the shortcomings of the existing voting system.

Keywords- Blockchain, voting, discrepancies, security, electronic voting, decentralized.

I. INTRODUCTION

The existing voting system consists of a lot of limitations as of now. During every voting season it's quite common to hear things like booth capturing, ballot box stuffing, tampering with the EVM machines, which is not ideal.

Hence, a need for a better voting system has emerged quite drastically. The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among various parties. Each transaction that is present in the blockchain is verified by most of the participants of the system.

The main feature of blockchain that we are going to access here is its immutability, which means data can't be altered or changed once it's saved in the records, so after the successful casting of the vote by a candidate, even if anyone gets access to all the records, he cannot manipulate the vote casted which makes it extra secure. Blockchain works by means of creating blocks of data with a particular identifier, to link the current block with the previous block the means of hashing is used.

Hashing takes a string of changing length to output a cryptic string of fixed length, by means of some mathematical algorithm. This generated hash is then used as an identifier within the next block of the blockchain, and hence links it to the previous block. A feature of hashed data is that it can't be traversed in the opposite direction, nor can it be decoded.

The proposed system will have an UI for voter/user and for the purpose of adding the vote, a function add Vote is called from the Voting UI. Since the hashing manner is a one-manner transaction, no one could be able to reverse it. Additionally, we have used the concept of decentralization, making it a completely decentralized blockchain voting platform.

II. LITERATURE REVIEW

Considering various types of requirements and after reviewing, proposed Votereum, [1] which is an electronic voting system based on the concept of blockchain. The system proposed is based on the ethereum blockchain platform which is open-source, decentralized and comes up with smart contract functionality.[1]

"Online Voting" The article [2] gives a fair share of ideas about the limitations of the current voting system. The article proved to be very useful in developing future voting platforms that would be free of all the limitations currently being encountered, and hence could play a huge role in the development of voting systems.[2]

David Khoury et al. proposed a decentralized voting system [3] based on the Ethereum blockchain in which main features of this system include ensuring data integrity and transparency, and enforcing one vote per mobile phone number for every poll that too with proper privacy. To accomplish this, the Blockchain runtime environment that has been used is Ethereum Virtual Machine.[3]

A Survey was done to reduce one of the cheating sources of the database manipulation, blockchains in databases of electronic voting systems has been proposed here, For encrypting data fetched from fingerprint sensor AES algorithm has been used. This research discusses the recording of voting results using blockchain algorithms from every place of elections.[4]

Friðrik Þ. Hjálmarson et al. created a system and a paper regarding potential of distributed ledger technologies such as blockchain and through the description of a case study has been evaluated. The agenda really is to host elections through electronic voting systems based on blockchain technology.[5]

Rifa Hanifatunnisa et al. described a recording system [6] which starts when the process of voting ends. One of the best and foremost solutions to solve the problems during the elections is the blockchain technology. Some of the features of this technology which makes it a lot more secure and reliable are-Usage of hash value to store the votes of different polling booths, and the presence of digitized signatures.

The sequence of steps proposed in this project makes sure that the voting system need not to go through the process of mining which is usually the specified case in the bitcoin technology as the voting details of a voter are saved only once and need not to be altered.[6]

III. LITERATURE SUMMARY

No	Paper	Algorithms
1	Survey on Blockchain Based E-Voting Recording System Design	a) Advanced Encryption Standard algorithm
2.	Online Voting: Voting System Using Blockchain	a) Cryptic Verification b) H.E.T Homomorphic Encryption Technique:
3.	Blockchain-Based E-Voting System	Quorum Geth: Go-Ethereum
4.	Blockchain Based Electronic Voting Record System Design	a) ECDSA-Elliptic Curve Digital Signature Algorithm b) SHA256 algorithm
5.	Decentralized Voting Platform Based on Ethereum Blockchain	a) HTML web-app through Apache Cordova b) Ethereum network
6.	Votereum:An Ethereum-based E-voting system	a) External Personal Account-EOA b) Contract Account c) Votereum

IV. LITERATURE ON E-VOTING AND THREATS

The constant development in technology also affects the whole process of voting and elections. With each advancement the developers are constantly trying to make their contribution to the system to make it more effective and beneficial for the society. They try to tackle the different factors like convenience, integrity of process, security and effectiveness in the latest designs so that the transition from the traditional methods of voting is seamless and rewarding.

There are plenty of problems that the election commissions face during the times of elections. To list some of the problems- duplicate voting, machine capture, forced voting, non-authentic voters voting and much more. Authentication is hence a significant feature that must really be present to ensure legal voting which is free of any kind of malpractices.

Voting done through the electronic means is a hot topic nowadays and it has proved to be a lot more beneficial than the traditional methods, but there is still a lot of scope for improvement in the electronic voting also. Some of the solutions provided for the security concerns are as follows-biometric verification, fingerprint, different encryption methods such as hashing and a lot more procedures are under study by the developers to overcome the present shortcomings of the voting system.

Electronic voting also known as E-voting sometimes is a means to conduct the voting process through the means of a digital platform. Since machines are involved in electronic voting, it is considered to be a lot more effective as it reduces the scope of human error. Now there are further two categories in E-Voting. In the first category the voting is done through the traditional ballots only but the counting of votes is done electronically.

In the second category the casting of votes and everything is done through electronic means only through the use of a machine of some kind through some graphical user interface usually. This mode is much more secure and much more effective than the first mode. Applications of E-Voting are immense. Some of the features that an effective e voting system must provide are as follows-:

1. Eligibility:
Authenticated, verified voters only can cast the vote.

2. Non-Duplicity:
No person can be allowed to vote more than once.

3. Incoercible Nature:
A voter must be free of being reprimanded about whom he cast his vote for.

4. Reliable Process:
Even during any kind of system failure,votes must remain secured.

5. Integrity:
Tampering of votes by anyone should not be allowed.

6. Verification:
It should be ensured that no mistake is done in counting of votes.

Now to end the discussion, in traditional voting systems there has to be a third party present for casting of votes, for counting of votes, which makes those systems a lot dependent on the integrity of the third party, if the third party does any kind of malpractice the voting system fails to meet its true result which is unbiased and secure voting. To tackle this issue, the decentralised feature of blockchain comes into the picture, so the dependency on the third party is completely removed.

Despite the fact that E-Voting is much more efficient much more feasible, it is still not used widely as the primary source of voting as it usually comes up with security issues in the casting and counting of votes but with the emergence of blockchain technology its much likely that the electronic voting system is going to be widely used worldwide as the primary source of voting very soon.

V. PREFATORIES BLOCKCHAIN

Blockchains are a type of data structures which are write only, which means you can put data into the blockchain's structure but you can't edit that entered data, you just aren't authorized to make any kind of changes to it. The structures that we talked about are known as blocks and are deployed in a point to point architecture. Each block of the blockchain is linked to the previous block through a cryptic function which is known as hash function, every block has the cryptic function of the previous block.

And hence, as one can imagine a chain of connected blocks is formed and this is why it is called as blockchain-Chain of blocks. That cryptic function which is called the hash function, provides various services such as-immutability, security, maintains integrity of data and much more.

New blocks in a blockchain are created through a process of mining, mining always adds the new blocks at the end of the blockchain Some of the significant features of blockchains include cryptography, transactions, blocks, smart contracts, peer to peer network. Each of these features are talked about in detail below-

1. Transactions and Blocks:
Every record or data after being added with a signature,after being verified and secured is rolled out into different blocks of blockchains and are termed as transactions. Thus, we can say each block of a blockchain contains transactions along with various fields such as timestamp and cryptic function of the previous block.

2. Cryptography:
It is one of the most significant aspect of a blockchain as it provides many valuable services like security, immutability, integrity, concept of hashing, protecting user data from any kind of malpractices.This is usually done through various hash functions which are very secure and very robust such as SHA1, SHA128, SHA256 etc.

3. Smart Contracts:
Smart contracts are nothing but processes which get executed automatically when a certain condition is met or reached. These are used to send data or values between different blockchain blocks without the need of any third party service.

4. Peer-to-Peer network:
What really is meant by peer to peer network is that there is no central power or central authority. And this is what blockchain actually is, it is a distributed system with no central organization or anything in power, everyone has equal authority.

Talking about the types of blockchains, there can be a couple of types of blockchains depending on various factors such as how data would be accessible, to whom data would be accessible, what are the allowed actions that a user could perform, namely- A Private Blockchain and A Public Blockchain.

What happens in a public blockchain is that the data present in the blockchain is accessible and is available to anyone, although certain parts of the blockchain might still be encrypted to ensure data integrity but most of it is public. In a public blockchain anyone can add a node or a block as per their need. Some of the examples of such blockchains are ethereum; bitcoin etc, as one can guess from this these types of blockchain form an essential part of economic welfare and status.

Now the private blockchain is quite the opposite of the public blockchain as in a private blockchain only a certain number of users or nodes are allowed to join the network. So this is a centralized infrastructure but not fully centralized as the distributed aspect also comes into the picture. In a private blockchain each node has defined permissions if it can mine data, run smart contracts or do transactions.

Unlike the usual decentralized concept of blockchain, this blockchain is governed by a central party called a trusted party. Private Blockchain is usually used for private works.

Some of the services provided by a blockchain node are:
- Get connected to the network.
- Making sure that the ledger is up to date.
- Actively ready for new transactions.
- Adding the verified transaction into the blockchain.
- Being ready or in a listening state for the arrival of new blocks.
- Validation of newly created blocks and confirmations of different transactions.
- Creation and adding of new blockchain blocks.

VI. PROPOSED SYSTEM

What we are trying to create here is a voting system which is different and a lot more secure than any of the voting systems that has ever came into practice uptil now.This voting system would be decentralized and hence no one governing authority would be there which really takes its integrity to a whole new level.

VII. PROJECT ARCHITECTURE

The architecture of the proposed system is given in the figure below. What each block does,what its functionality is, has been depicted by the respective interconnections.
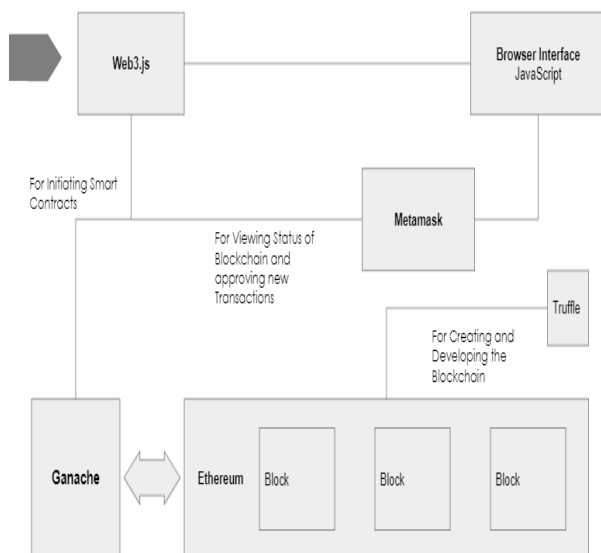

Fig 1. Project Architecture.

Lets take it step by step.The first thing would be to verify the voter's identity, whether he is a legal voter or not so that any other country person doesn't end up voting, whether he is what he says he is or not so that someone else may not vote on behalf of someone else, these are some of the concerns that the first step tackles up with.

To check for all this we would be using various identity card numbers and recognition devices to get to know whether the voter is present in the database or not,whether he/she is a legal voter or not.

After the first step is done each voter is provided by a unique hash address which is then used to cast the vote at a unique address,each hash address is associated with ethers which makes sure only one vote is cast at each hash address. So to sum up the whole process,the voter on the day of the voting will come to the booth and go through different security checks,after that he/she will be provided with a unique hash address using which he would cast the vote and then log out of the system.
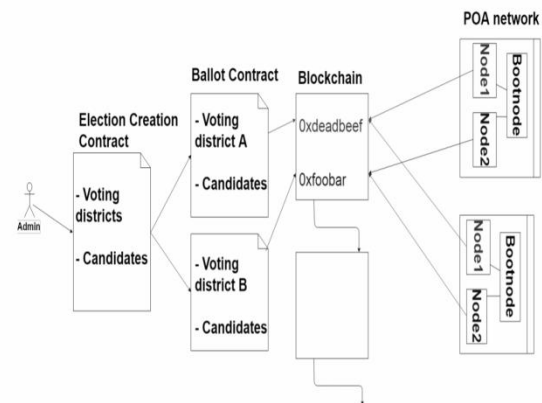

Fig 2. Election as a smart contract.

The system that we have proposed will work as the best substitute for the modern voting systems that are being used such as EVMs.Our proposed system would be D-app whose frontend would be made with different languages like html, css javascript etc, for the backend different technologies would be there like nodejs web3js and a couple of frameworks like ganache and truffle,the language used for the smart contracts would be solidity.

Details of the voter would be mentioned in the smart contract.one of the most logical most significant piece of the entire code would be the smart contracts.As we talked about earlier, contents of the blocks are termed as transactionsSo every changes that we would make, will reflect in the transactions.Transactions are in fact a way for the outside world to come in contact with the ethereum network.

Anytime we wish to make any kind of state changes or any kind of updation in the blockchain,a transaction would be used.Now the tricky part is that these transactions just doesn't work for free,they require a service charge,a currency for their execution,and this is where the ethers come into picture.Ethers act as a type of currency for the transactionsHere in our proposed system we are using Ganache which sets up the blockchain nodes and everything almost immediately. Metamak would be utilized to run the decentralized apps directly in the browser without actually running the whole ethereum node.

REFERENCES

[1] Votereum: An Ethereum-based E-voting system: Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao and Tuan A. Nguyen, "Votereum: An Ethereum-based E-voting system", 2019, University of Information Technology Vietnam National University HCMC, Vietnam.

[2] Online Voting: Voting System Using Blockchain: Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar,

"Online Voting: Voting System Using B-chain", 2019.

[3] Decentralized Voting Platform Based on Ethereum Blockchain: David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb, 2018, "Decentralized Voting Platform Based on Ethereum Blockchain", Department of Computer Science American University of Science and Technology.

[4] Survey on Blockchain Based E-Voting Recording System Design: G Bhavani "Survey on Blockchain Based E-Voting Recording System Design", 2018.

[5] Friðrik Þ. Hjálmarson, Gunnlaugur K. Hreiðarsson, "Blockchain-Based E-Voting System", 2018, School of Computer Science Reykjavik University, Iceland.

[6] Blockchain Based E-Voting Recording System Design: Rifa Hanifatunnisa and Budi Rahardjo, 2017, "Blockchain Based E-Voting Recording System Design".

[7] Emre Yavuz; Ali Kaan Koç; Umut Can Çabuk; Gökhan Dalkılıç (2018) towards secure e-voting using ethereum blockchain.

[8] David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb,(2018), Decentralized Voting Platform Based on Ethereum Blockchain

[9] Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao and Tuan A. Nguyen,(2019), Votereum: An Ethereum-based E-voting system.

[10] Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar, "Online Voting: Voting System Using B-chain", (2019), Online Voting: Voting System Using Blockchain.

[11] Design: Rifa Hanifatunnisa and Budi Rahardjo, (2017), Blockchain Based E-Voting Recording System.

[12] Supriya Thakur Aras, Vrushali Kulkarni, (2017) "Blockchain and Its Applications – A Detailed Survey", International Journal of Computer Applications, Pune, India.

[13] Venkata Naga Rani B, Akshay S, Arun kumar M , Ishwar Kumar M A , (2019) , Decentralized E-Voting System,International Research Journal of Engineering and Technology

[14] Dipali Pawar, Pooja Sarode, Shilpa Santpure, Poonam Thore. Implementation of Secure Voting System using Blockchain ISSN: 2278-0181, Vol. 9 Issue 06, June-2020

[15] Xu, Min & Chen, Xingtong & Kou, Gang. (2019). A systematic review of blockchain. Financial Innovation. 5. 10.1186/s40854-019-0147-z.

[16] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 463-467, doi: 10.1109/IC3I.2016.7918009.

[17] H. R. Andrian, N. B. Kurniawan and Suhardi, "Blockchain Technology and Implementation: A Systematic Literature Review," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 2018, pp. 370-374, doi: 10.1109/ICITSI.2018.8695539.

[18] Dabbagh, Mohammad & Sookhak, Mehdi & Safa, Nader. (2019). The Evolution of Blockchain: A Bibliometric Study. IEEE Access. PP. 1-1. 10.1109/ ACCESS.2019.2895646.

[19] Kitsantas, Thomas & Vazakidis, Athanasios & Chytis, Evangelos. (2019). A Review of Blockchain Technology and Its Applications in the Business Environment.

[20] Ashish Singh,Kakali Chatterjee," Secure Electronic Voting System Using Blockchain Technology",2018 International Conference on Computing, Power and Communication Technologies (GUCON) Sep 28-29, 2018.

[21] Ghiro, Lorenzo & Restuccia, Francesco & d'oro, Salvatore & Basagni, Stefano & Melodia, Tommaso & Maccari, Leonardo & Lo Cigno, Renato. (2021). What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things.

[22] Redshaw, Tom. (2021). Cryptocurrencies and Blockchains. New Media & Society. 14614448219 9999. 10.1177/1461444821999995.

[23] Takaoğlu, Mustafa & Ajlouni, Naim & Ozyavas, Adem. (2021). A Survey of Artificial Intelligence Driven Blockchain Technology: Blockchain Intelligence.

[24] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigData Congress.2017.85.

[25] Mohanta, Bhabendu & Jena, Debasish & Panda, Soumyashree & Sobhanayak, Srichandan. (2019). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. 8. 100107. 10.1016/j.iot.2019.100107.

[26] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[27] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.

[28] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.

[29] Hanifa Tunisia, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017.

[30] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.