Telecom Business Review
15 (1) 2022, 17-22
http://publishingindia.com/tbr/

Blockchain-Based Decentralized Voting System

Shrey Garg*, Simran Chauhan, Deepak Kumar***, Saroj Kumar Manna******

**School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India.*
Email: 2018009679.shrey@ug.sharda.ac.in

***School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India.*
Email: 2018014397.simran@ug.sharda.ac.in

****School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India.*
Email: 2018014480.deepak@ug.sharda.ac.in

*****School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India.*
Email: 2018000901.saroj@ug.sharda.ac.in

Abstract

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

Keywords: Blockchain, Voting, Discrepancies, Electronic Voting, Decentralized

Introduction

The existing voting system consists of a lot of limitations as of now. During every voting season, it's common to hear things like booth capturing, ballot box stuffing, and 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 cast which makes it extra secure. Blockchain is a ledger that connects blocks of data with a unique identifier and links all previous blocks to the current blocks with hashing. Hashing is a function that is used to solve blockchain computation using cryptic methods. This created hash result goes as an identifier within the subsequent blocks of the blockchain. Hence links it to the successive block. A feature of hashed data is that it cannot be accessible in the backward direction.

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

Literature Review

Considering various types of requirements and after reviewing, proposed Votereum, (Choudhari et al., 2019) 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 (Choudhari et al., 2019).

"Online Voting" The article (Khoury et al., 2018) 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 (Khoury et al., 2018).

David Khoury. proposed a decentralized voting system (Bhavani et al., 2018) based on the Ethereum blockchain, which main features include ensuring data integrity and transparency and enforcing one vote per mobile phone number for every poll with proper privacy. To accomplish this, the Blockchain runtime environment that has been used is Ethereum Virtual Machine (Bhavani et al., 2018).

A Survey was done to reduce one of the cheating sources of the database manipulation; blockchains in databases of electronic voting systems have 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 creation (Yavuz et al, 2018).

Friðrik Þ. Hjálmarson. created a system and a paper regarding the potential of distributed ledger technologies such as blockchain and evaluated through the description of a case study. The agenda really is to host elections through electronic voting systems based on blockchain (Hjálmarson et al., 2018).

Rifa Hanifatunnisa described a recording system (Hanifatunnisa et al., 2017) that starts when the voting process ends. One of the best and foremost solutions to solve the problems during the elections is blockchain technology. Some of the features of this technology that make it a lot more secure and reliable are: the usage of the hash value to store the votes of different polling booths and digitized signatures. The sequence of steps proposed in this project ensures that the voting system does not need to go through the process of mining, which is usually the specified case in bitcoin technology, as the voting details of a voter are saved only once and need not to be altered (Anasune et al., 2019).

E-Voting and Trends

The constant technological development 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 society. They try to tackle the different factors like convenience, the integrity of the process, security, and effectiveness in the latest designs so that the transition from traditional voting methods is seamless and rewarding (Xu et al., 2019).

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 voting, and much more. Hence, authentication is a significant feature that must be present to ensure legal voting, which is free of malpractices (Pawar et al., 2020). Voting done through electronic means is a hot topic nowadays and has proved to be a lot more beneficial than the traditional methods, but there is still a lot of scope for improvement in electronic voting. 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 (Linh Vo-Cao-Thuy et al., 2019).

Electronic voting, also known as E-voting, is a means to conduct the voting process through 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 two further categories of E-Voting. In the first category, the voting is done through the traditional ballots, 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 (Venkata et al., 2019).

Applications of E-Voting are immense. Some of the features that an effective e-voting system must provide are as follows:

- *Eligibility:* Authenticated, verified voters, only can cast a vote.
- *Non-Duplicity:* No person can be allowed to vote more than once.
- *Incoercible Nature:* A voter must be free of being reprimanded about whom he cast his vote for.
- *Reliable Process:* Even during any kind of system failure, votes must remain secured.
- *Integrity:* Tampering of votes by anyone should not be allowed.
- *Verification:* It should be ensured that no mistake is made in the counting of votes.

Now to end the discussion, in traditional voting systems, there has to be a third-party present for the 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 decentralized 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, it's much likely that the electronic voting system is going to be widely used worldwide as the primary source of voting very soon (Çabuk et al., 2018).

Prefatory Blockchain

Blockchains are a type of data structure that is write-only, meaning 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 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 the hash function, and every block has the cryptic function of the previous block. And hence, as one can imagine, a chain of connected blocks is formed, which is why it is called a blockchain-Chain of blocks. That cryptic function, called the hash function, provides various services such as immutability, security, maintaining the integrity of data, and much more.

New blocks in a blockchain are created through a process of mining, and mining always adds the new blocks at the end of the blockchain (Gopi et al., 2019). Some of the significant features of blockchains include cryptography, transactions, blocks, smart contracts, peer to peer networks.

Each of these features is talked about in detail below:

- *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, each block of a blockchain contains transactions along with various fields such as timestamp and cryptic function of the previous block.
- *Cryptography:* It is one of the most significant aspects of a blockchain as it provides many valuable services like security, immutability, integrity, concept of hashing, and protection of user data from any malpractices. This is usually done through various hash functions which are very secure and very robust such as SHA1, SHA128, SHA256 etc.
- *Smart Contracts:* Smart contracts are nothing but processes that 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 for any third-party service.
- *Peer-to-Peer Network:* What really is meant by the 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.

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, and what the allowed actions 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 available to anyone; although certain parts of the blockchain might still be encrypted to ensure data integrity, most of it is public. In a public blockchain, anyone can add a node or block per their need. Examples of such blockchains are Ethereum, bitcoin, etc. From this, these types of blockchain form an essential part of economic welfare and status (Agbesi et al., 2019).

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 (Patidar et al., 2019). Unlike the usual decentralized concept of blockchain, this blockchain is governed by a central party called a trusted party. A private blockchain is usually used for private works.

Some of the services provided by a blockchain node are:

- Get connected to the network.
- Make 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.

RESULT

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

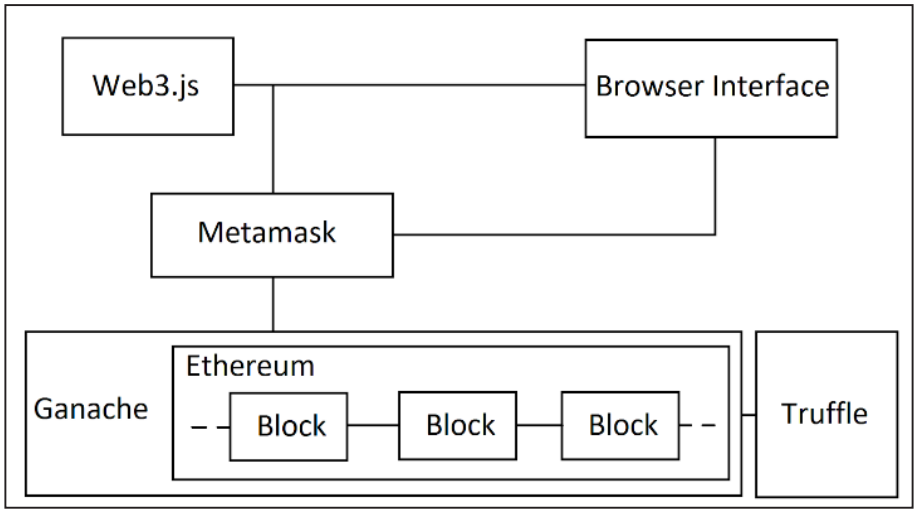
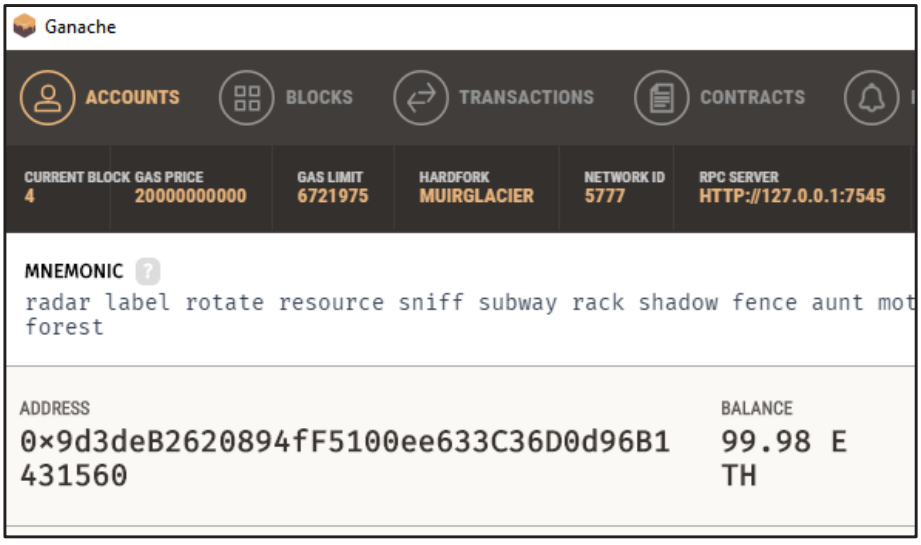
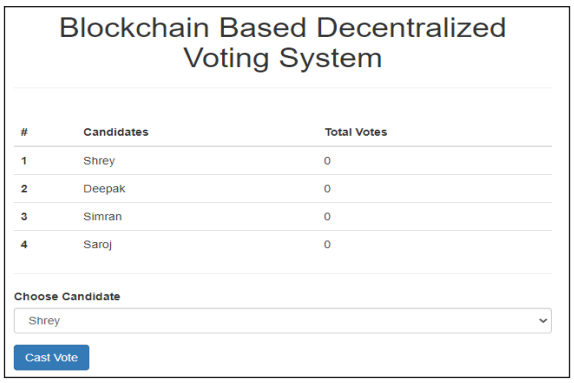


Fig. 1: Project Architecture



Source: TruffleSuite.

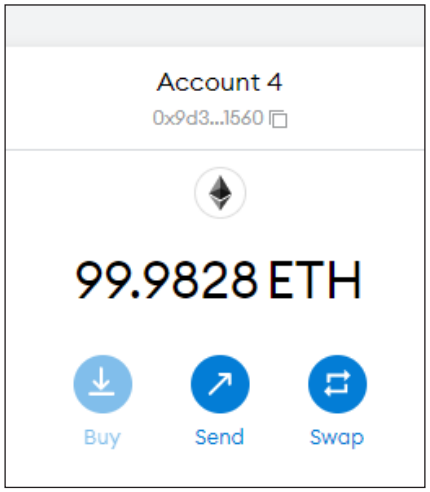
Fig. 2: Ganache Interface with an Active Ethereum Blockchain and One Account Visible



Source: Google.

Fig. 3: Front-End Interface

Let's 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 and whether he/she is a legal voter or not. After the first step, each voter is provided with a unique hash address, which is then used to cast a vote at a unique address; each hash address is associated with ethers, ensuring 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 a vote and then log out of the system.



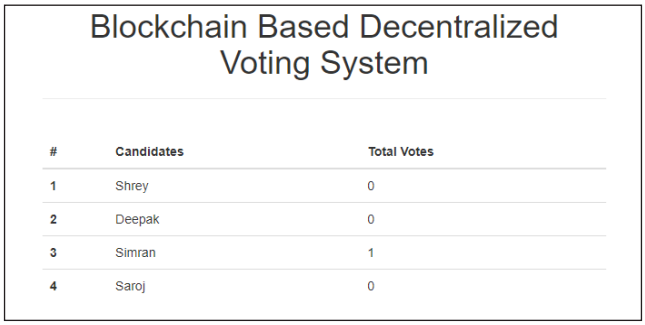
Source: Google.

Fig. 4: Metamask with Imported Account

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 a D-app, whose frontend would be made with different languages like HTML, CSS, JavaScript etc., for the different backend technologies would be there like Web3js and a couple of frameworks like Ganache and Truffle, the language used for the smart contracts would be the solidity. Details of the voter would be mentioned in the smart contract. one of the most logical, most significant pieces of the entire code would be the smart contracts. As we discussed earlier, the blocks' contents are termed transactions.

So, every change we 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 state changes or updates in the blockchain, a transaction would be used. Now the tricky part is that these transactions don't work for free, they require a service charge and a currency for their execution, and this is where the ethers come into the picture. Ethers act as a type of currency for transactions.

Here in our proposed system, we use Ganache, which sets up the blockchain nodes and everything almost immediately. Metamask would be utilized to run the decentralized apps directly in the browser without actually running the whole Ethereum node.



Source: Google.

Fig. 5: Vote Transaction Completed Successfully

CONCLUSION

As fascinating as the idea of adopting a voting system in elections may seem, it is quite evident that many enhancements are to be made to the existing ones before we can even think of testing them, let alone using them in the elections. India is the world's largest democracy, and

there is no proper sense in using a faulty voting system in such a vast democracy; it would just lead to more and more problems in the road ahead.

Keeping in mind the enhancements required and the faults present in the existing voting system, we have developed a voting system based on blockchain technology. This paper discusses all the major faults and enhancements that are required to make voting in the largest democracy in the world feasible. In this paper, an in-depth analysis has been made using many sources to get aware of the developments and steps required to implement those features.

Throughout this paper, efforts have been made to provide efficient research on the topic of blockchain and its application in the digital voting system. Some aspects of the blockchain, like decentralization, have been given special focus to understand and implement the concepts more clearly and efficiently. The problem of malpractices like vote tampering has been discussed, and solutions have been provided to tackle the problem.

The work to implement all the features discussed is also underway, and with time new enhancements will also be added to the application.

Acknowledgments

In the end, we would really like to appreciate every single person who has helped in the development of this paper at any point in time. A special thank you to our guide Dr. Rani Astya for her valuable input and guidance. Last but not least, thank you, Sharda University, for providing us with a platform to showcase our work. Without your help, it wouldn't have been possible.

References

Choudhari, P., Kelapure, M., Halgaonkar, P., & Shirke, P. (2019). Online voting: Voting system using B-chain.

Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018). Decentralized voting platform based on Ethereum blockchain. Department of computer science American University of science and technology.

Bhavani, G. (2018). Survey on blockchain based E-voting recording system design.

Hjálmarson, F. Þ., & Hreiðarsson, G. K. (2018). *Blockchain-based E-voting system*. School of Computer Science Reykjavík University.

Hanifatunnisa, R., & Rahardjo, B. (2017). Blockchain based E-voting recording system design.

Yavuz, E., Koç, A. K., Çabuk, U. C., & Dalkılıç, G. (2018). Towards secure e-voting using Ethereum blockchain.

Anasune, V., Choudhari, P., Kelapure, M., Halgaonkar, Shirke, P., & Halgaonkar, P. (2019). Online voting: Voting system using blockchain.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*(1). doi:https://doi.org/10.1186/s40854-019-0147-z

Pawar, D., Sarode, P., Santpure, S., & Thore, P. (2020, June). Implementation of secure voting system using blockchain. *International Journal of Engineering Research & Technology (IJERT), 9*(6), 1595-1598.

Vo-Cao-Thuy, L., Cao-Minh, K., Dang-Le-Bao, C., & Nguyen, T. A. (2019). *Votereum: An Ethereum-based e-voting system.* University of Information Technology Vietnam National University HCMC.

Venkata N., B., Akshay, S., & Kumar, A., & Kumar, I. M. A. (2019). Decentralized e-voting system. *International Research Journal of Engineering and Technology, 6*(3), *8040-8050.*

Çabuk, U. C., Adıgüzel, E., & Karaarslan, E. (2018). A survey on feasibility and suitability of blockchain techniques for the E-voting systems. *IJARCCE, 7*(3), 124–134. doi:https://doi.org/10.17148/IJARCCE.2018.7324

Gopi, S., Giridharan, B., Mohamed Rifoy, R., Sivachidambaram, S., & Yuvaraja, S. (2019). Effective in-house voting and implementation using blockchain verification. *International Research Journal of Engineering and Technology, 6*(3), 8088-8092.

Agbesi, S., & Asante, G. (2019, November 29). *Electronic voting recording system based on blockchain technology*. 12th CMI Conference on Cybersecurity and Privacy, CMI.

Patidar, K., & Jain, S. (2019). *Decentralized E-voting portal using blockchain.* Inspec Accession Number: 19277744 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT).