

E-voting Powered by Blockchain

Rajat Kumar¹, Dhanajit Kapali², Abhijeet Kumar³, Himanshu Rawat⁴, Jayant Kumar⁵

¹ Assistant professor, Department of Computer science and engineering, Dronacharya Group of Institutions, Greater Noida, UP, India

^{2,3,4,5} B. Tech, (CSE), Dronacharya Group of Institutions, Greater Noida, UP, India.

ABSTRACT

Blockchain is a new-age technology which provides various digital services. As it is still emerging, besides its benefits or to make it more reliable, it is talked about for its legal issues. Here, we are using Blockchain technology to develop an E-voting System which can make elections economical and easy to conduct. This technology will provide full security and trustworthiness between the public and authorities.

Keywords: Blockchain, blocks, nodes.

I. INTRODUCTION

When the first electronic voting system was introduced in nations like Norway, Switzerland. It was not easy for it to compete with the old and known Ballot System. It has to provide a more secure and authentic way of voting that can build trust and belief among the public so that they can vote without any fear and hesitation of influences, and tampering of casted votes. Also, it does not provide anonymity to the voter. As to counter all the above we developed an E-Voting System using Blockchain technology.

II. LITERATURE REVIEW

Method In this paper [2], it has highlighted the major problem in voting security where in the 2016 US Presidential Elections, EVM's were likely to be intercepted and votes were tampered. The study found that this old voting equipment is prone to failures and crashes, also they are notoriously easy to hack and tamper with. In this study [3] by Ayed, Ahmed, et al., it has been proposed an electronic voting system based on the Blockchain technology. The system is decentralized which ensures security. Any registered voter can cast a vote using any device connected to the Internet. The Blockchain will be available publicly and can be easily verifiable. It will be distributed in a way that no one will be able to corrupt it. Rifa and Budi have found that the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable if we use hash values in recording. In the blockchain the use of the sequence proposed for the chain creation process considers that in an electoral system it is not required for mining as in the Bitcoin system, the proposed sequence ensures that all nodes is legally connected can avoid collision in transportation [4]. Bin, Joseph, et al., has come to a conclusion that the current blockchain voting system cannot provide the comprehensive security features, and most of them are platform dependent, we have proposed a blockchain-based voting system that the voters' privacy and voting correctness are guaranteed by homomorphic encryption, linkable ring signature, and PoKs between the voter and blockchain [5].

The main demerit of e-voting is that regarding the security of this process, The source code has hidden essential parts of code which no one can trust or check the accuracy as it can be manipulated by corrupt election commission or other international entities at any time as they can have complete access to source code for which many people demanded for a better way. To make it completely open-source and transparent, enlisting every voter with their identity credentials but some people were concerned about their privacy as it can lead to political tensions between people and leak of data too on a national level.

This amount of data being leaked can create a serious advantage to many enemy countries as their citizens' information can be used in a several number of ways.

To counter these problems, the system we are going to propose in this paper will address all these security concerns by using open-source code and Ethereum app platform to develop our e-Voting system, and based on Blockchain technology to secure votes, and decentralize the system.

III. What is Blockchain

Model blockchain is a decentralized, distributed, and oftentimes public, digital ledger consisting of records called *blocks*. In simple words blockchain is a database that stores encrypted blocks of data then chains them together to form a chronological single-source-of-truth for the data. Blockchain works on (DLT) distributed ledger technology. It syncs with the ledgers remotely replicated among multiple servers by using community or mutual validation, which is appointed to serve as the public transaction ledger like Ethereum based cryptocurrency. Miners take time to hash data and then the hash keys are pointed to remote nodes, information is stored on various nodes and hash behaves as their servers point to the next node for serialized data retrieval. This chain structure provides stability and security to our data and hackers cannot access the data by breaching a random node. The data on the other hand compromises the information each transaction.

IV. Proposed System

We are going to propose an e-voting system in this paper which will be powered by blockchain. It addresses all the security concerns by using open-source code and Ethereum app platform. To develop our e-Voting system, we rely on Blockchain technology to secure votes, and decentralize the system.

V. Our solution implements the below requirements

- All The voters should be anonymous. There should be no link between the ballots and the voter's identity. Their anonymity should be kept even after the election.
- No duplicate votes should be present. The Counting of Votes must be accurate.
- The system should be verifiable to ensure the correct count of votes.
- People who are registered as voters should only be allowed to cast a vote. Our system will not support any registration process.

VI. Use of Blockchain

The first block will be a foundation block. It will be created in the first transaction which will represent the candidate. It will act as a base block for every further transaction. Every new transaction will count as a new vote for it. The first transaction will not be counted as a valid vote and it will only contain the name of the candidate.

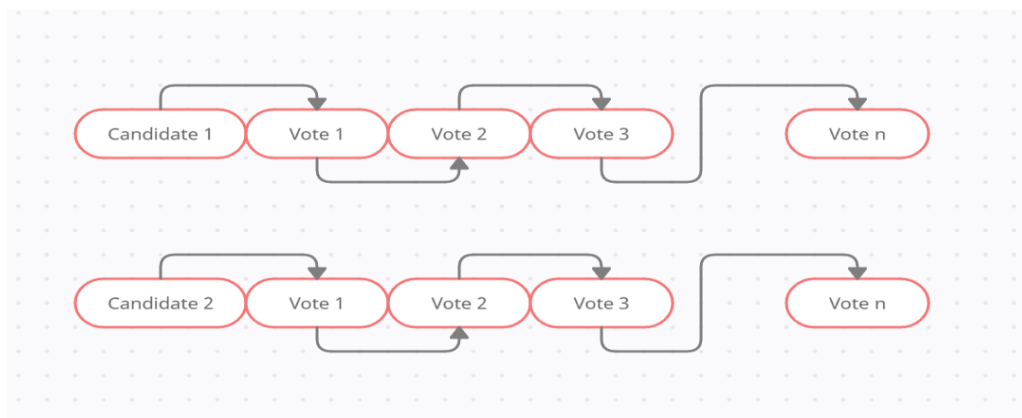


Figure 1: Creation of blockchains for each candidate

Each block will use the previous voter's information to create its hash code, this will ensure the security of the votes. Since all the blocks are connected, if any block is compromised then it will be identified immediately. The blockchain is decentralized so corrupting it will be very hard. The actual voting is done at the blockchain. There are multiple nodes in the whole blockchain network, and the user's vote will be sent to any of these nodes and they will add the vote in the blockchain.

VII. Representation of the blockchain voting system

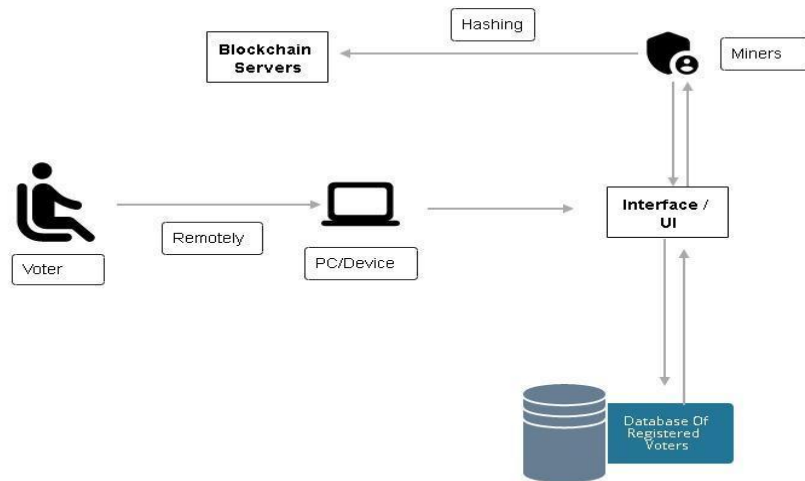


Figure 2: E-voting Flow

- 1) **Requesting to vote:-** The user should be able to log in to the voting system after successful verification of his voter's id. The voter needs to use a unique account in the e-voting system which will be created only if the voter persists a valid voter id. Our system will not allow any voter to themselves generate their own identities to register to vote.
- 2) **Casting a vote:-** After successful registration of voters in our e-voting platform, the voter can cast a single vote on any of the listed candidates. Our system will prevent any voter from casting multiple votes.
- 3) **Encrypting votes:-** After the voter casts his vote, a transaction will be initiated to store his vote in the blockchain in the form of a block. His voter id and the hash of the previous block will be used to generate the hash of this block, this way each input will be unique and ensure output to be unique and encrypted as well.
- 4) **Adding vote to the blockchain:-** After a successful vote, a block will be created which will be attached to a blockchain according to the candidate selected by the voter and each block will get linked to the previously casted vote.

VIII. Concusses in the blockchain

With a decentralized system, the problem of concussions may occur. In our system, it may happen too. This problem occurs when multiple votes are cast approximately at the same time. To resolve this issue, we will use the longest chain rule. This rule is also used in Bitcoin. Let us suppose all the blocks in our system are synchronized and the chain is at block 2001. Now suppose three new votes have been cast at the same time and now they all should be assigned as block 2002. We will call these blocks 20021-A, 2001-B, 2001-C.

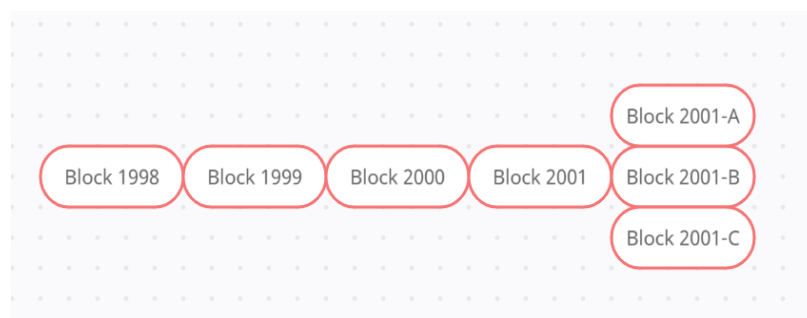


Figure 3: Multiple Blocks arriving blockchain at same

Now let us assume that block 2001-A was introduced first to the blockchain, so the system will add it in the chain as a successor block of block 2001. Later on, block 2001-B will arrive, now the system will keep a hold of it and wait for another block. Now, say block 2002-A is introduced to the system, the blockchain will assume

that block 2001-A is the valid block and keep building on the longer chain. Block 2001-B and 2001-C will be considered orphan blocks.

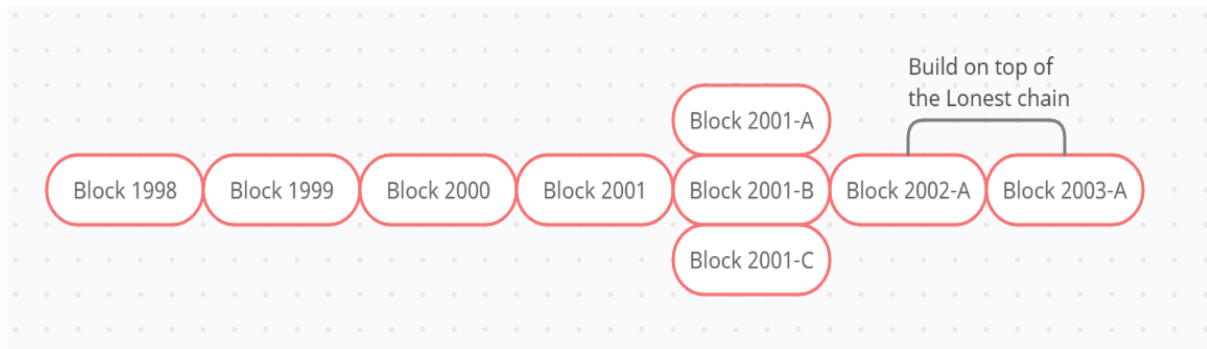


Figure 4: Building Chain Using Longest Chain Rule

Since we have a different chain for each candidate, orphan blocks will not cause any issue as they can be later counted as valid votes.

IX. Conclusion

We have proposed an online voting platform based on blockchain technology. The system is decentralized ensuring security. The blockchain will be publicly available and verifiable.

Any registered voter will be able to cast a vote if his device is connected to the internet. We have also illustrated the limitations of our system which will be addressed in the future research papers.

X. References

- [1] A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting Ruhi Ta,s 1,2,* and Ömer Özgür Tanrıöver 1
- [2] BLOCK CHAIN TECHNOLOGY FOR ELECTRONIC VOTING ONG KANG YI1, DEBASHISH DAS2* 1Asia Pacific University of Technology & Innovation (APU).
- [3] Blockchain-Based E-Voting System Friðrik
- [4] Crypto-Voting, a blockchain based e-voting system Francesco Fusco 1, Maria Ilaria Lunesu, Filippo Eros Paniand Andrea Pinna 2.
- [5] Benny, Albin, Blockchain based E-voting System (July 11, 2020).