International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain Based Decentralized Voting System

Ashay Sahare[1], Agrey Srivastava[2], Ashwika Dethe[3], Bhavishya Ambrish[4], Shounak Rushikesh Sugave[5]

[1,2,3,4]Dept. of Information Technology, MIT College of Engineering, Pune, India
[5]Associate Professor, School Of CET, MIT World Peace University, Pune, India

---

Abstract - *The success of any democracy depends on the fairness of its elections. Building a secure voting system that maintains secrecy of votes while still providing transparency to the voters has been a challenge for a very long time. The recent rise in malpractices such as EVM tampering and booth capturing has raised questions regarding the integrity of the election process. This has forced the authorities to look for new secure ways to conduct elections. In the recent years the advancements in the web technology have led to the development of decentralized networks. These networks are considered to be more secure as opposed to the traditional centralized frameworks. One such application of decentralized networks which has gained popularity in the recent years is Blockchain. In this paper we propose a novel peer to peer system based on Blockchain in order to process and store the EVM transactions. The proposed model also tries to address various problems of the current system.*

***Key Words*: Blockchain, Election EVM, P2P Network, Decentralization, Voting Machine, Proof of Work**

1. INTRODUCTION

Election is the backbone of any democracy. Every citizen in the nation has equal right to contribute towards the decision-making process. Therefore, preserving the integrity of the election process is very important. A nation needs a fair and unbiased election process for people to make the most out of their right to elect the leader of their choice.

Traditionally elections were conducted using a ballot paper where voters marked the candidates of their choice and submitted the ballot papers at the voting stations. These ballot papers were then manually counted which resulted in a huge delay in the election process. Although this method of conducting elections was fairly simple, it did not scale well. Manual counting of votes wasn't practical for large scale elections and was very time consuming. Replacing this pen and paper with a new electronic system had the potential to limit fraud and make the voting process traceable and verifiable [1].

This problem was tackled by the Election Commission of India with the introduction of Electronic Voting Machines (EVMs) in the late 1990s. These machines were exclusively produced by a group of government agencies namely Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL). These devices were cheap, easy to use and had a simple design. As a result, EVMs were widely adopted throughout the country.

Even though the machines were believed to have a simple design, the actual working mechanism of the EVMs has not been made completely public. Due to this, the EVMs have been subjected to widespread criticism by various political parties who questioned their integrity and reliability. Recently there has also been increase in the allegation of electoral frauds regarding the EVMs such as the 2009 parliamentary elections. This has raised various concerns in the minds of the citizens regarding the electoral procedure in the country. Along with this, even though the Electronic Voting Systems significantly reduce the time required for the election process, there is still some amount of manual counting involved. To acquire the the final vote count, the EVMs from all the regions are taken to a secure location and the votes are tallied in the presence of the representatives of all the political parties [2].

As a result of this, the authorities have been forced to look for other reliable alternatives to the standard electronic voting systems. The idea of I-Voting (internet voting) has gained popularity in the last few years as a viable solution to the current system. The concepts of i-voting address various issues faced by the traditional system; however, it does not provide enough transparency to the voters. Moreover, the principle of secret suffrage through internet voting has significant issues when compared to EVMs [3]. Blockchain is robust, immutable and trusted technology that contains blocks of data linked using cryptography. Blockchain was originally developed by Satoshi Nakamoto [4] as a medium to secure online transactions. Various features of the blockchain such as proof of work and decentralization using peer-to-peer networks make it more secure than any other record keeping structure. Due to this Blockchain is considered by many, including us as a highly secure method of storing data. In this paper we propose a hybrid system that is based on the structural framework of a conventional voting system while still utilizing the added security features offered by the modern I-voting systems.

2. MOTIVATION

Due to the inherent simplicity of the EVMs it is very easy to tamper the machines. Most of the attacks on EVMs are physical in nature [2]. Anyone with the basic knowledge of

electronics can disturb the mechanism of the EVM which in turn could disrupt the entire election process. Recent studies have also shown that access to the EVMs for a few minutes is enough to tamper the mechanism of the machine [5]. Current day voting system faces challenges related to security of votes and usage of EVMs. The detailed security analysis of the EVMs was done was Scott Wolchok [2]. Some of the key findings from his study are discussed below:

- Corrupt hardware can be attached to the voting machine and it can be manipulated easily. This results in favouring a particular candidate at the time of voting.
- Replacing the Original device with a malfunctioned one so that every time a vote is given to a candidate it goes to a particular candidate instead of the intended one.
- The EEPROM chip of the EVM can be replaced with another chip with corrupted count of votes in favor of each candidate which can be a problem to detect.

3. RELATED WORK

Blockchain technology was initially implemented by Satoshi Nakamoto [4] in 2008 to imbibe the concept of cryptocurrency (or) bitcoins as a medium of secure exchange of money. Since then researchers have been trying out different ways in which blockchains can be used, from storing healthcare records or using it as a criminal database for national security. One such application of blockchains is in electronic voting systems. In [6], a Blockchain based solution for voting is proposed but the implementation is not discussed. A smart contract for boardroom voting with maximum voter privacy [7] proposed the very first practical use of decentralized and self-tallying online voting system with the help of blockchain called as the open vote network. Similarly, Arya Sahadevan and his team members [8] were able to develop an IOT based system to deal with the issues and flaws of polling booths. In another research, Agora : a voting system was proposed as a solution for government which as based on end to end verifiable blockchain by using a token based system [9]. In [10], a centralized authentication server (CAS) is used and a decentralized blockchain based model is used to store the votes.

4. BLOCKCHAIN TECHNOLOGY

Blockchain is a technology which is used for securing digital transactions and storing information related to those transactions. The digital information (Block) is stored in a public database which is called the 'Chain'. Block stores the information about the transactions like time, date and other details related to the transaction which includes who is initiating the transaction and to whom it is intended for. It grows and stores records in each block by attaching the new block to the chain, hence the name "Blockchain".

When the block is added, it is assigned a cryptographic hash code for its unique identification. Every block contains hash code of previous block, timestamp, transaction data and hash code of block itself. Due to this arrangement when a change is made in a block it results in change in hash key of that particular block which creates a mismatch between current block key and the key stored in the next block. Thus, it results in a broken chain. The basic structure of a blockchain is shown in Fig1.

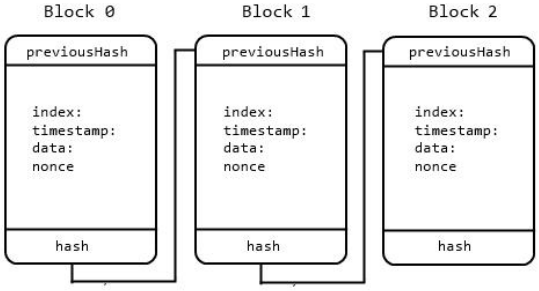

Fig -1: Structure of a blockchain

In Blockchain, hashing is used to join the block to the chain. The process involved in hashing is an irreversible process which makes it nearly impossible to retrieve the actual (original) data from the hash itself. Even a small change in data is reflected in the hash key which is generated for each block. The reasons which provides such high level of security to blockchains is the fact that blockchain is a decentralized system i.e. data is distributed over all the nodes and in order to change it and reflect an actual change, data needs to be changed in every node which is nearly impossible.

Depending on the scope of the application, blockchains can be of following types [11, 12]:

- *Public:* It is a permissionless blockchain in which any user can join by simply creating an address. All users have permission to read as well as write to the blockchain. In a public blockchain the users can decide if they want to become a miner or simply run as a node in the system.
- *Private:* It is a permissioned blockchain which is controlled by a central authority. In a private blockchain only authorized participants are allowed to join the network, view the transactions and validate them.
- *Consortium:* It is also a permissioned blockchain. It is similar to a private blockchain except that the permissions are controlled by a group of individuals or organizations instead of a centralized authority.
- *Hybrid:* It is a combination of permissioned and permissionless blockchain. It combines the security of public blockchains and the speed of private blockchains to form a hybrid structure.

The steps involved in order to make a transaction in the network are listed below [13]:

1. The node creates a transaction with details such as timestamp, data, hash of the current block etc. and sends it to all the nodes in the network.
2. The nodes with high computing power called the miners validate the transactions using consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS) etc.
3. The transactions which are validated are used to create a new block containing the block index, block timestamp, list of transactions, previous hash, and hash of the current block.
4. This block is then transmitted to all the nodes and added to the chain.

5. PROPOSED MODEL

In this paper we propose a reliable, efficient and highly secure way of storing the votes. In the current system, the EVMs rely on its hardware for the most part. The model proposes extended use of software in order to leverage the security features of e-voting and combine it with the robust architecture of the current system. This results in a hybrid system that is secure as well as highly scalable. However, in order to do so we need a way to connect the EVMs together in a network. This makes the EVMs vulnerable to a number of network-based attacks such as man-in-the-middle, DDoS, session hijacking, receipt stealing etc. The solution to these problems is to make use of decentralized architecture as opposed to the conventional centralized models thus eliminating the centralized points of failure. The model proposes the use of a private (permissioned) [12] blockchain that allows only the identified EVMs to connect to the network and interact with it. This protects the system from malicious devices that may try to interfere with the voting process. The design mainly consists of following four main components:

5.1 Verification Subsystem

The verification subsystem interacts with the voter database to verify voter's credentials. The database also consists of a status flag that indicates if the voter has previously voted or not. This helps to ensure that the voter is not allowed to vote multiple times. Initially, the status will be false or not voted for all the voters. Although a blockchain based database can be used to further improve security against double voting, the time required to search a blockchain based database increases linearly with the number of blocks. In most countries there already exists a database that contains data of its citizen, it is convenient to integrate these government databases with the system instead of creating a new database from scratch.

5.2 Controller Station

Each EVM works in coordination with a controller station. The controller station acts as the bridge between the verification subsystem and the EVMs. It is used to fetch the voter's information from the verification subsystem and feed the required input fields to the EVM. Its main task is to verify the voter's identity and prepare the EVM for the vote to be registered.

5.3 Broker Service

The broker acts as a discovery service by EVMs discover other nodes in the network and connect to them. The broker service acts as a connection manager that keeps real-time track of the nodes entering and leaving the network. Every time a new node is connected to the network, the broker service provides it with a list of all the active nodes in the network so that it can initiate connections to them. It then adds the metadata of the incoming node to the list of active nodes. When a node leaves the network, the broker notifies all the nodes in the network to terminate connections with the leaving node.

5.4 EVM Network

All the EVMs in the network are connected to each other in the system to form a full mesh network. Any two nodes in the network communicate with each other using a duplex bidirectional data stream, thus forming a peer to peer network. EVM nodes are able perform a number of operations on the blockchain like registering votes, creating new blocks, fetch newly created blocks from other nodes in the network and request latest instance of the blockchain.

6. SYSTEM DESIGN

Fig. 2 represents the basic architecture of the system consisting of a single EVM node:

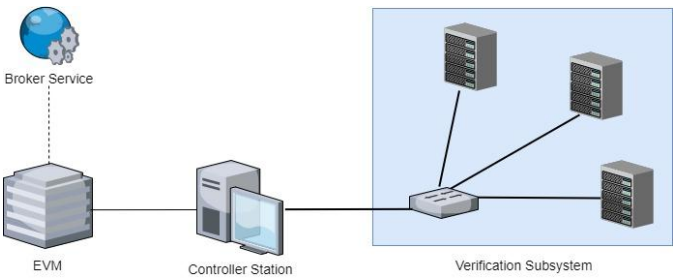

Fig -2: Architecture of the proposed model

When the EVM is booted up, the first step it needs to perform is to connect to the peer to peer network of the EVMs. In order to do this, it sends a request to the broker service to provide the credentials of the active nodes in the network. The broker service then returns the metadata of all

the nodes in the network essential to establish connections with them. On receiving this response from the broker, the EVM can then initiate connections to all the nodes in the network. After successfully connecting to the network, the broker service adds the metadata of the new node to the list of active nodes in the network. This information can then be used by the next incoming nodes in the network to connect to this EVM. The EVM is now ready to interact with the blockchain. The first operation that every node needs to perform after connecting to the network is to fetch the latest instance of the blockchain. The EVM is then ready to initiate the voting process.

Each EVM in the network is interfaced with a controller station which is used to switch the EVM between locked and unlocked state. The EVM cannot interact with the blockchain when it is in the locked state. When the voter arrives at the voting booth, the voter interacts with the officials present at the controller station where the identity of the voter is manually verified by the authorities. The officials then enter the voter's information at the controller station from where it is sent to the verification subsystem to fetch other information about the voter. The verification subsystem searches the voter's databases in order to retrieve the voter's information. This information also includes the flag that indicates if the voter has already voted. This information is then sent back to the controller station where this information is manually checked again. If the status flag is false or not voted, then the controller station forwards the voter's information to the EVM and signals the EVM to switch to the unlocked state. The EVM is now ready to register vote for the provided voter-id. The voter then proceeds to the EVM and presses the button corresponding to the candidate of his choice. Upon successfully registering the voter's input, the EVM notifies the voter that the vote is successfully cast and the EVM goes back to the locked state. This notification can be as simple as a blinking LED light. The voter can then exit the voting booth and the process can be repeated for the next person.

Each vote registered by the EVM is kept in a list of pending transactions to be added to the blockchain. As an additional security measure to provide vote secrecy to the voters, the votes are encrypted before they are added to the block. By encrypting the votes in the chain, it is impossible for anyone to trace the votes back to the voters. After a fixed interval of time (called as mining cycle) a new block consisting of all the pending transactions is created. Along with the pending transactions the newly created block contains other information such as timestamp, hash of the previous block in the chain, node-id of the EVM that has created it, etc. This block is then sent to all the nodes in the network for verification.

Upon receiving a block from any EVM in the network, each node performs a set of verification actions in order to validate the incoming block. Various checks that are used to validate the block include ensuring the block's hash is correct and matches the standards specified by the authorities. It is also checked that the block's data produces the correct hash value contained in the block's structure. The underling transactions contained by the block are also checked in order to check if the block contains any invalid or fraudulent votes. To improve the security against double voting, an additional layer of protection can be added where all the previous blocks in the chain are traversed in order to check if the voter-id of any transaction in the incoming node has already been encountered before. The incoming block is discarded if it fails to pass in even one of these checks. If all the checks are passed and the block is successfully validated, then the block is added to the blockchain.

7. CONCLUSION

In this paper, a security mechanism based on blockchain technology has been designed to be integrated with the EVMs in order to maintain the integrity of votes in the election process. Suitable modifications to the original implementation of the blockchain by Satoshi Nakamoto [4] has been suggested to suit the requirements of a voting system. Since the proposed design makes use of a decentralized network, when any malicious change is made to the votes stored in the blockchain then the chain tampering is noticed and the tampered block is replaced with the correct one from another randomly chosen node in the next mining cycle thus protecting the data from modifications. In order to successfully modify the data stored in the blockchain, the change needs to be reflected at the data stored in all the nodes in the network. Along with this, the data stored in all the subsequent blocks at all the nodes will also have to be changed to maintain the cryptographic link between all the blocks. In this way our model can ensure the integrity of the votes at all times.

8. FUTURE WORK

In future it is planned to develop security measures for the system to resist attacks like Denial of Service (DDoS) which may affect various layers in the network stack. It is also intended to upgrade the model to handle enormous number of connected nodes in the network. The model can further be optimized to reduce the time taken for block verification. Alternative methods like biometric authentication as explained in [14] can also be added to further improve the overall security of the system. This would also help to reduce the human intervention required in the process. A SMS based notification system can also be implemented in order to notify the voters on their registered mobile phones that the block containing their vote is added to the blockchain. Building on top of this, the hash of the block containing the user's vote can be provided using which the voters can verify their votes using an OTP mechanism. In practical cases, where the number of nodes in the network might be very large; certain modifications can be made to the

system. One such change would be to add a congestion flag that can be used to protect the nodes from being overwhelmed by the incoming verification requests. Or in case of network congestion, the verification request can be forwarded to another uncongested node.

REFERENCES

[1] Nicholas Weaver, "Secure the vote today," Available at: https://www.lawfareblog.com/secure-vote-today

[2] Wolchok, et al. , "Security analysis of India's electronic voting machines," Proceedings of the 17th ACM conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010.

[3] Adrià Rodríguez-Pérez, "Secret suffrage in remote electronic voting systems", Fourth International Conference in eDemocracy & eGovernment (ICEGEG) pp. 227-228.

[4] Satoshi Nakamoto, "Bitcoin: a peer-to-peer electronic cash system." Available at: http//bitcoin.org/bitcoin.pdf

[5] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, "Blockchain-based e-voting system," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA.

[6] Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, "A privacy-preserving voting protocol on blockchain", IEEE 11th International Conference on Cloud Computing, 2018.

[7] Patrick McCorry, Siamak F. Shahandashti, Feng Hao, "A smart contract for boardroom voting with maximum voter privacy," Financial Cryptography and Data Security, 2017, Volume 10322.

[8] Arya Sahadevan, Deepa Mathew, Jairam Mookathana, Bijoy Antony Jose, "An offline online strategy for IoT using MQTT," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing.

[9] Agora (2017), "Agora: Bringing our voting systems into the 21st century", Available at: https://www.agora.vote

[10] Sagar Shah, Qaish Kanchwala, Huaiqian Mi, "Block chain voting system," Northeastern University, 2016.

[11] Mahdi H Miraz and Maaruf Ali, "Blockchain enabled enhanced IoT ecosystem security," Int. Conf. on Emerging Technologies in Computing 2018 (iCETiC'18), London Metropolitan University, London, UK.

[12] Daniel Dob, "Permissioned vs Permissionless Blockchains: Understanding the differences," January 7, 2020. Available at: https://blockonomi.com/permissioned-vs-permissionless-blockchains/

[13] Sobti, Rajeev & Ganesan, Geetha, "Cryptographic Hash Functions: A review," International Journal of Computer Science Issues (2012), Volume 9 p461-479.

[14] Yirendra Kumar Yadav, Soumya Batham, Mradul Jain, Shivani Sharma, "An approach to electronic voting system using UIDAI", 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Coimbatore, India, February 13-14, 2014.