ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse45932020.pdf
https://doi.org/10.30534/ijatcse/2020/45932020

E-Voting system using Blockchain technology

Aishwarya Indapwar[1], Manoj Chandak[2],Amit Jain[3]
[1, 2]Shri Ramdeobaba College of Engineering and Management, Nagpur,
Maharashtra, India, [3]Velocity Technology solution, Pune.
*indapwarag@rknec.edu, hodcs@rknec.edu,amit.jain@velocity.com

ABSTRACT

Nowadays, normal voting using EVM(Electronic voting machine) which stores the votes of each voter in a centralized database. And after researching many different e-voting applications, most of the application used centralized data storage as the database. As, these centralized databases stores the complete data at a single location and is easy hackable and can be tampered with. Hence, due to this the data can be inconsistent while voting count and will not provide us with the correct result.Hence, using blockchain technology, we create a decentralized application where the tampering of data becomes almost impossible as Blockchain uses the decentralized algorithm for the data storage where the data is stored at a single location.

The main objective of E-voting system using blockchain is to create a e-voting system underneath using a blockchain technology. This system is just like a normal voting system, of which same process is conducted on e-voting which used to be conducted on the normal paper-based voting with the use of mobile, web browser for the voting purpose by the voters. Therefore, this paper will give a review of blockchain technology and how this technology will be used in E-voting system.

Key words: Bitcoin, Blockchain technology, cryptographic function, Decentralized application, digital signature, distributed ledger technology (DLT), E-voting, hashing, Merkle tree, time stamp.

1. INTRODUCTION

To construct a secure electronic voting system is a difficult task.The US Pentagon had proposed the online voting system in year the 2005, but this system does not work well due to lack of legitimacy of votes.[1][2]Hence, to come up with an application which is less hackable and in which data cannot be tampered we can used blockchain technology in an e-voting application. Blockchain is the revolutionary way of stored data in a decentralized way and has many future applications.

1.1 Blockchain

Blockchain has become an important technology in all the fields. Blockchain is a decentralized and distributed ledger technology that records the provenance of a digital asset. Blockchain is sometimes referred as distributed ledger technology (DLT) that makes any digital asset transparent with the help of decentralization and cryptographic hashing. An easy example to explain blockchain technology is the Google Doc. When wecreate a document and shared with many people, this document will get distributed rather than copying and transferring. This creates a decentralized distributed chain that can provide access to everyone at the same time. [3] No one will wait other party for making changes and all this modification will be recorded in real time which are transparent to everyone. However, blockchain is more complicated than a Google Doc but the concept is same.Blockchain is said to as a promising technology as it helps to reduce risk, eliminate fraud and brings transparency in a scalable way.[2][5] Blockchain has a distributed database that maintains an ever-growing list of data records secured for tampering. Also, it is decentralized that avoids a single point failure which may occur in centralized systems.

As the name indicates blockchain is chain of blocks where each block is linked with other using cryptography. Blockchain consists of two cryptographic keys that are private key and public key. These keys help to perform successful transaction between two parties. Each person has two keys which is used to produce a secure identity reference. This identity is referred as digital signature and is used for controlling transactions. [4] Each block consists of a cryptographic hash value of the previous block, a timestamp and transaction data. For using distributed ledger, blockchain manages peer-to-peer network which helps in inter-node communication and validating new blocks. The structure of blockchain is shown in figure 1:

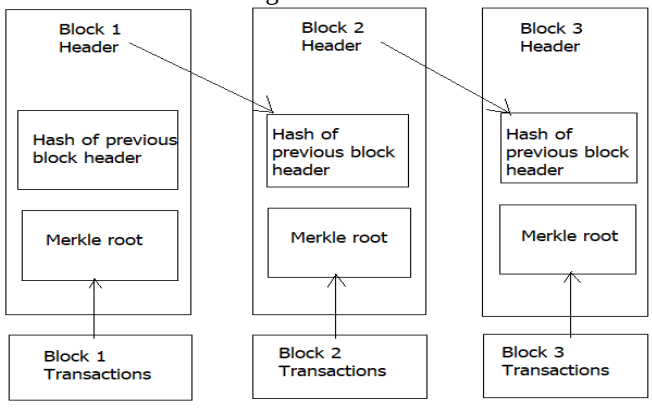

Figure 1: Structure of blockchain

- Blocks: As shown in figure 1 every chain consists of multiple blocks. Each block holds a transaction that are hashed and encoded into a Markle tree. Each block contains a cryptographic hash of previous block and the link of blocks form a chain like structure.Each block contains digital signature, a time stamp and other relevant information. [8][7]It should be noted that the block does not include identities of individuals, this block is transmitted across all network and when right person uses his private key and matches it with block the transaction gets successful. Each block consists of three basic elements, data in a block, a 32- bit whole number called as nonce and a 256-bit number called as hash. Blockchain technology uses hash encryption to secure data mainly SHA256 algorithm to secure information. This nonce will be generated randomly when a block is created. The hash is extremely small and it must start with huge number of zeroes. When the first block is created, a nonce generates the cryptographic hash.

- Miners: Miners creates new blocks on chain through the process named as mining. In blockchain every block contains unique nonce and hash, but it also refers the hash of previous block in the chain. So, mining a block is not an easy task especially on large chains. A special software is used to solve the complex math problem of finding nonce that generate hash. As the nonce is only 32 bit and the hash is 256, there are almost four billion combinations that are mined before the right one is found. When a block is mined successfully, the change is accepted by all nodes on network.

- Nodes: In blockchain technology no one computer can own the chain. Instead, it is distributed with the help of nodes connected to the chain. Nodes can be of any kind such as an electronic device that maintains copies and keeps network functioning.

1.2 Challenges in Voting system

- Privacy: The voter is allowed to view only his details and to whom voted. The only disclosed information in election is total votes in entire election.

- Lack of evidence: There is no evidence that the votes that are being casted is under effect of bribes or any other fraud.

- Scalable: Elections must be flexible enough to work at large scale also.

- Speed: It must be ensured that the election result should be declared within few hours of procedure ends.

- Low cost: Cost is one of the major factors for any system design. The system must be cost efficient.

1.3 E-voting using blockchain

Blockchain has become important in almost all the fields but one of the most valid domains is voting.[12] To construct a secure electronic voting machine is a difficult task as it is a crucial system that must be executed without failure.The advantages of e-voting using blockchain includes:

- Greater transparency due to open and distributed ledgers
- Inherent Anonymity
- Security and Reliability(especially against Denial of service attacks)
- Immutability(strong integrity for the voting scheme and individual votes.)

Blockchain distributes the information of votesto thousands of computers that makes impossible to alter or delete votes once they have been cast. This method promotes greater trust between voters and governments by protecting their data.[8] Blockchain will allow all to cast their votes on smartphone or from the computer with the apps, rather than having a queue at polling stations. Implementing blockchain will not require a government to change their existing system rather their existing platform can be re-modelled.[11] The major weakness of blockchain is that it can handle a small string of text that simply record a balance transfer between two parties. However, Interplanetary file system (IPFS) provides much of the infrastructure needed for the blockchain content storage as it provides permanent decentralized web and no central entity controls the data.

2. LITERATURE REVIEW

In this section, we introduce study done by few researchers.[1] QuocKhanh Nguyen, Quang Vang Dang proposed a review paper on BlockchainTechnology for theAdvancement of the Future. This article gives an overall view of Blockchain technology and its potential to contribute to the development of the future by proposing several directions for further research. This paper proposed the effects of industrial revolution 4.0 to the society were robots will replace humans completely in the work force. This paper explains the basic operation of blockchain technology that is peer-to-peer decentralized ledger which provides a method to record and distribute information publicly on peer-t-peer systems of computers through crypto protocol. This paper also describes the advantages of blockchain such as it is arranged rationally that allows user to execute quick insurance requests that can be valuate immediately using AI and Blockchain decentralization helps it become less likely to be attacked. It gives role of blockchain in technological revolution 4.0 and also within the society. Blockchain can help in faster insurance and payments, it can make travelling easier by helping the travel insurance agencies to automate payment which saves a great amount of time, helps in protecting corporate identities, in banking sectors, internet

security, supply chain management, helps government to alleviate bureaucracy, increase safety and transparency in government activities and many more. [2]Hussein Hellani, Abed EllatifSamhat, Maroun Chamoun, Hussein El Ghor, Ahmed Serhrouchni proposed a review paper On Blockchain Technology: Overview of Bitcoin and Future Insights. This paper investigates bitcoin cryptocurrency application and blockchain technology that enables existence of digital currency. This paper also highlights requirements and benefits related to security, database and network. This paper gives the understanding of Bitcoin as it is a peer-to-peer electronic cash system. The word bitcoin denotes three different objects: blockchain platform, digital currency and protocol that runs over this platform to define how transactions are moved. This paper describes the characteristics of blockchainwhere the distributed ledger is structured into two main network types: permission less network such as bitcoin where anyone can join the network without previous permission. Participants of this type can validate the transaction and might be part of the consensus and block creation and the permissioned network which is a private network limited to a number of trusted entities that got permission to join the network in order to validate transactions. Microsoft recently deployed blockchain as a service called Ethereum consortium blockchain.

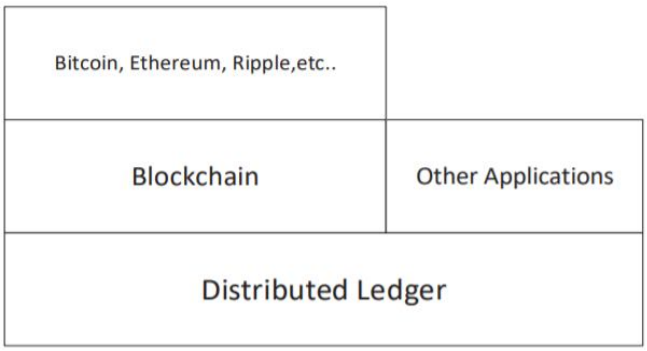

Figure 2: Distributed Ledger topology

Figure 2 shows the distributed ledger topology were distributed ledgers improve security and efficiency in the businesses especially for a company that deals with unknown or new customers. A blockchain is a type of a distributed ledger, comprised of unchangeable timestamps records by hashing them into an ongoing chain of hash-based proof-of-work, digitally recorded data in block of transactions that are validated by consensus mechanism based on the online data of distributed ledger. [3]Rifa Hanifatunnisa, Budi Rahardjo a review paper on Blockchain Based E-Voting Recording System Design. This research discusses the blockchain technology used to record the voting results from every place of election. This paper suggests that blockchain technology is one solution that can be used to reduce the problems that occur in voting. This paper illustrates the uses of blockchain as it is timestamped, programmable and highly available. This paper proposed a design of a database recording system on e-voting using blockchain.

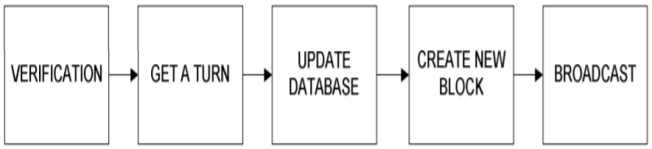

Figure 3 : Flow chart design

Figure 3 is the flow chart design proposed for blockchain technology where they proposed a system in which the process begins when the voting process at each node has been completed. Before the election process begins, each node will generate a private key and a public key. Public key of each node sent to all nodes, so each node has a public key list of all nodes.Once valid, then the data will be added to the database in the block.After the database is updated, the node will check that thenode ID that was brought as a token is his or not. [4] Ahmed Ben Ayed proposed a review paper A conceptual secure blockchain-based electronic voting system. They proposed an e-voting system that includes four main requirements such as authentication where people who are already registered can cast a vote, this system supports a registration process, anonymity where e-voting system should not allow any links between voters identities and ballots, accuracy where every vote is unique and every vote should be counted and the verifiability where system should be verified to make sure all votes are counted correctly. Beside all these main requirements it also provides solution that supports mobility, flexibility and efficiency. In this proposed system the first transaction added to the block will be a special transaction that represents the candidate. When this transaction is created it will include the candidate's name and will be treated as thebase block, where every vote for that candidate is placed on top of base node. Unlike the othertransactions, the base node will not be counted as a vote, and it will only contain the name of thecandidate.Every time a person votes the transaction gets recorded and the blockchain will get updated. To ensure that the system is working correct, the block will contain the previous voter's information. If anyone of the blocks is failed, then it would be easy to find out since all blocks are connectedto each other.The vote casted be the user is sent to that specific candidate's node, and the node then adds the vote to the Blockchain. The voting systemwill have a node in each district where the election is held to ensure the system is decentralized.The drawback in this system is that it is assumed that voters will use a secure device to cast their vote. Even while this system is secure, the hackers have the ability to cast or alter a vote using malicious software already installed on the voter's device. One of the drawbacks of this system is the inability to change a vote in case of auser mistake. The user will be able to cast their vote only once.

3. REPRESENTATION OF THE E-VOTING SYSTEM

Using blockchain technology, we can create a decentralized application where the tampering of the data becomes almost impossible as blockchain uses the decentralized algorithm for the data storage where the data is not stored at a single location.[9] Hence, to come up with an application which is

less hackable and in which data cannot be tampered we used blockchain technology in the voting application. Figure 4 explains how the e-voting system works. The steps to implement e-voting system:

- Setting up the environment for blockchain technology: For setting up the environment, the research has to be done as there are many different multiple frameworks for blockchain technology. These frameworks include Hyperledger, Ethereum, multichain, etc. This project will include the use of Ethereum framework for setting the environment for blockchain. Ethereum provides the complete implementation of blockchain technology, so that the complex work of creating the complete blockchain is not required and more focus is on building the application.
- Download the NodeJS setup file from the site and install on the system. NodeJS is a JavaScript framework which provides the development environment for Ethereum framework. Now install the basic files and packages.
- Creating smart contract for e-voting system: Blockchain stores blocks of data in the ledger. Each block of data contains multiple transactions. These transactions are verified by the smart contract before getting stored in the blocks of blockchain ledger. If not verified, the transactions cannot be added onto the block. The smart contract is written in solidity language. Remix is a platform which provides a platform to check whether the smart contract contains any error or not.
- Testing the smart contract on remix.
- Creating the authentication interface for 2 modules manager and voter using ReactJS and using Firebase for the authentication purpose.
- Creating UI for manager where election can be created by adding new parties with their member name and an UI to show the results of the election.
- ReactJS is used for creating UI for authentication of both the modules. It uses Firebase as a No-SQL database for the database of voter and manager.
- The UI for manager module and voter module is created. The manager module will hold functionality for adding members name and parties to the election and showing the results of the election. The voter module is used for voting hence the UI of voter module contains only the name of the parties and an option to vote. Whenever a voter votes, a transaction is generated to which confirmation is needed. After the confirmation, the vote is added and counted.

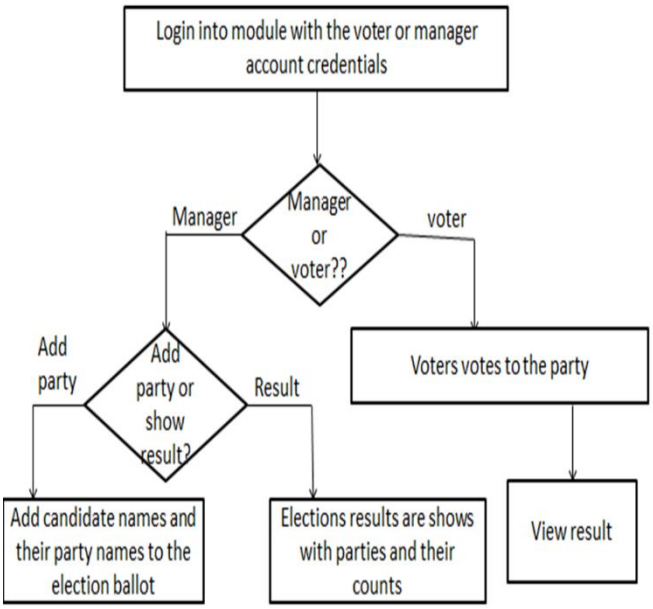

Figure 4: Flowchart of e-voting system

3.1 Technology used for E-voting

- Metamask:

Metamask allows the user to visit the distributed web of future in your browser today. It also allows to runEthereum in your browser without running a full Ethereum node.It includes a secure identity block, that provides a user interface to manage their identities on different sites and sign blockchain transactions.

- NodeJS:

NodeJS is an open source, cross-platform environment for developing server-side and networking applications. NodeJSapplications are written in JavaScript, and can be run within the NodeJS on OS X, Microsoft Windows, and Linux. It also provides a collection of various JavaScript modules which makes the development of web applications using NodeJS easier to a great extent.

- ReactJS:

ReactJS is a JavaScript library that is used for building various reusable UI components. It creates UI components, which can present data that changes over time. Lots of people use React as V in MVC. React offers a simpler programming model and gives better performance. React can also be built on the server using node, and it can charge native apps using React Native. React implements one-way reactive data flow, which reduces the boilerplate and is easier to reason about than traditional data binding.

4. CONCLUSION

A permissioned, public, shared blockchain is a form of hybrid system that provide for situations where whitelisted access is required but all the transactions are viewable by the public. This will provide transparency that is needed in democracies.

E-voting however can bring some new problems such as ensuring privacy especially in the case of public permission less blockchains but there are solutions for that. Other problems include the speed by which the transactions can be verified. So blockchain technology may be championed as the solution to may problems but one domain where it might make sense in the end is electronic voting system.

REFERENCES

[1] Quoc Khanh Nguyen, Quang Vang Dang**. Blockchain Technology for the Advancement of the Future,** 4th International Conference on Green Technology and Sustainable Development (GTSD), January 2018.
https://doi.org/10.1109/GTSD.2018.8595577
[2] Hussein Hellani, Abed EllatifSamhat, Maroun Chamoun, Hussein El Ghor, Ahmed Serhrouchni. **On BlockChain Technology: Overview of Bitcoin and Future Insights,** IEEE International Multidisciplinary Conference on Engineering Technology (IMCET),2018.
https://doi.org/10.1109/IMCET.2018.8603029
[3] Rifa Hanifatunnisa, Budi Rahardjo. **A review paper on Blockchain Based E-Voting Recording System Design,** 11th International Conference on Telecommunication Systems Services and Applications (TSSA),2017.
https://doi.org/10.1109/TSSA.2017.8272896
[4] Kanika Garg,PaviSaraswat,Sachin Bisht, Sahil Kr. Aggarwal, Sai Krishna Kothuri, Sahil Gupta. **A Comparitive Analysis on E-Voting System Using Blockchain,** 4th International Conference on Internet of Things: Smart Innovation and Usages, 2019.
https://doi.org/10.1109/IoT-SIU.2019.8777471
[5] Ahmed Ben Ayed.**A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM,** International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.
https://doi.org/10.5121/ijnsa.2017.9301
[6] S. Nakamoto.**Bitcoin: A Peer-to-Peer Electronic Cash System**, www.Bitcoin.Org, p. 9, 2008.
[7] A. G. Malvik and B. Witzoee. **Elliptic Curve Digital Signature Algorithm and its Applications in Bitcoin**, pp. 1–5, 2016.
[8] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3. **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**, IEEE 6th International Congress on Big Data, 2018.
[9]Fridrik p. Hjalmarsson, Gunnlaugur K. Hreidarsson. **Blockchain-Based E-Voting System**, 2018.
https://doi.org/10.1109/CLOUD.2018.00151
[10] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb. **Decentralized Voting Platform Based on Ethereum Blockchain**, IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018.
https://doi.org/10.1109/IMCET.2018.8603050
[11] JulijaGolosova, Andrejs Romanovs. **The Advantages and Disadvantages of the Blockchain Technology**, 2018 DOI 978-1-7281-1999-1/18.
[12] A. Barnes, C. Brake, and T. Perry. **Digital Voting with the use of Blockchain Technology**,Team Plymouth Pioneers – Plymouth University, 2016.