ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

Survey on Blockchain Based E-Voting Recording System Design

G Bhavani

Department of E & TC, N B Navale Sinhgad College of Engineering, Solapur, India

ABSTRACT: Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system; there is one organization that manages it. Some of the problems that can occur in traditional electoral systems is with an organization that has full control over the database and system, it is possible to tamper with the database of considerable opportunities. Blockchain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. For encrypting data fetched from fingerprint sensor we are going to use AES algorithm. This research discusses the recording of voting result using blockchain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this thesis proposed a method based on a predetermined turn on the system for each node in the built of blockchain.

I. INTRODUCTION

Special in that it doesn't contain a reference to a previous block. Once the genesis block has been initialized 'Block 1' is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root. The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header, this means to change data you would have tomodify the block that records the transaction as well as all following blocks, as seen in Figure 1.

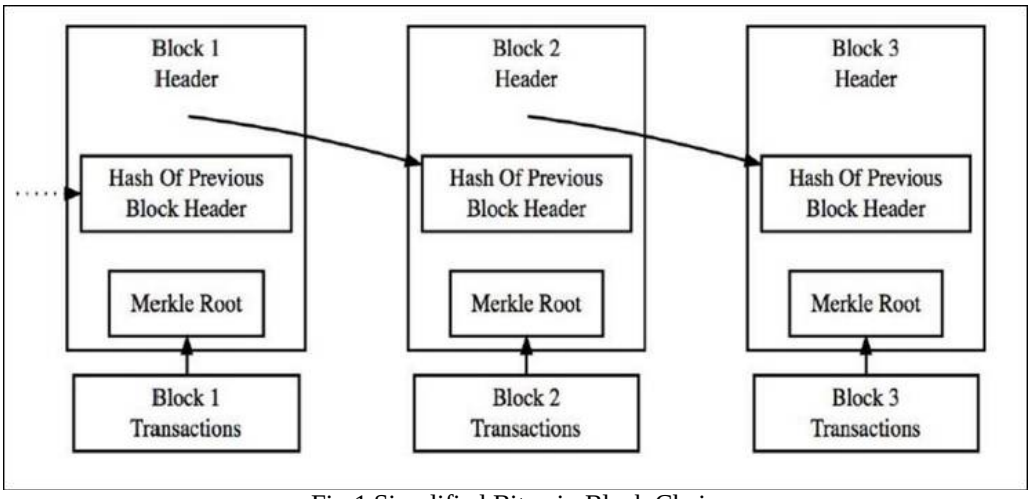

Fig 1 Simplified Bit coin Block Chain

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

A blockchain is designed to be accessed across a peer-to-peer network, each node/peer then communicates with other nodes for block and transaction exchange. Once connected to the network, peers start sending messages about other peers on the network, this creates a decentralized method of peer discovery. The purpose of the nodes within the network is to validate unconfirmed transactions and recently mined blocks, before a new node can start to do this it first has to carry out an initial block download. The initial block download makes the new node download and validate all blocks from block 1 to the most current blockchain, once this is done the node is considered synchronized.

II. LITERATURE SURVEY

The utilization of the grouping proposed in the blockchain creation process in this framework considers that in a constituent framework not required for mining as in the Bitcoin framework in light of the fact that the voter information and numbers are clear and are not permitted to choose more than once, the proposed succession guarantees that all hubs Which is legitimately associated and can maintain a strategic distance from impact in transportation. Likewise ensure all hubs that have enrolled the outcomes are incorporated into the figuring procedure. As far as expense can likewise be more effective on the grounds that it doesn't require hardware that is dependably changed in every race did. In light of the structure and the consequences of research led, it very well may be presumed that the framework is effective usefulness of chronicle the e-casting a ballot framework dependent on Blockchain innovation. [1]

A blockchain is a common, appropriated, and permanent record. The blockchain has produced serious enthusiasm for use in an assortment of enterprises and areas, going from saving money, back, and protection to medicinal services, government, retailing, and assembling. Associations are utilizing blockchains to grow new applications that are more solid and proficient. In this paper we investigate the blockchain innovation for building PC data frameworks. We first direct a methodical investigation of uses and issues identified with blockchain innovation, and after that distinguish a few issues that require additionally look into with the end goal to be legitimately tended to. We additionally examine the potential use of blockchain in instruction, and how training frameworks can profit by the coming of blockchain innovation [2]

The utilization of innovation has turned out to be typical now in addressing human needs. The expanding utilization of innovation has acquired new difficulties the procedure of majority rule government as a great many people today don't confide in their administrations, making decisions essential in current vote based system [3].

Races have an incredible power in deciding the destiny of a country or an association. Basic motivation behind the decision is the diverting of mainstream sway as a delegate majority rule government. Each voter who likes to come to surveying stations and shows voter cards to the panel and decision bosses to demonstrate whether the decision is substantial or not, after the calamity as an authentic alternative then the council gives a vote to the decision of organic sound votes settled on by casting a ballot in the decision of letter sound, at that point crease the vote and place it in the tallying station. The vote check in customary races can take 3 to 7 working days relying upon the speed of sending the sound to a more elevated amount [4]. At each phase of the vote include that is the aggregate arrangement of votes or not. The most continuous issue in decisions is the issue of information control, security, and straightforwardness.

The bitcoin [5], or, in other words and most well known digital currency, has been accepting a great deal of consideration. One of its specialized highlights is that it empowers solid exchanges without an incorporated administration component regardless of whether there are untrustworthy members in the system, and this element is gotten by the innovation of blockchain innovation. A blockchain is something like a record in which the sum total of what exchanges have been recorded, and it is shared by the members of a bitcoin organize. The structure of a blockchain is that a square that comprises of various exchanges is associated with a past square in chain-like frame. To guarantee dependability, when another square is added to the past square, a little exceptional procedure of understanding a riddle, called evidence of-work, is required and this riddle isn't simple. This is on account of this procedure can keep assailants from producing the blockchain all alone. With the quantity of bitcoin exchanges getting to be bigger and bigger, talk of blockchain applications other than those for cash has been pushed [6] into the spotlight. This is on account of the unwavering quality of the innovation has been kept up notwithstanding when it is put to use on a substantial scale. Some of the time the methodology of these applications that exploit the highlights of blockchain is classified "bitcoin 2.0".

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

With the improvement of innovation, the utilization of innovation in beating the issues that happen winds up critical, and in addition the complexities of the accumulation procedure [7]. Security is dependably the greatest worry for an e-casting a ballot framework. There ought to be no e-casting a ballot framework to anchor information and ought to have the capacity to withstand potential assaults. Blockchain innovation is one arrangement that can be utilized to decrease the issues that happen in casting a ballot. Blockchain has been utilized in Bitcoin exchange database frameworks [8]. Blockchain is disseminated, unchangeable and straightforward record who can't deny reality [9].
Comprises of a few hinders that are connected to one another and in arrangement. The square is connected in light of the fact that from the past hash utilized in the following square making procedure, the endeavor to change the data will be more troublesome as it needs to change the following squares [10]. The database was made open, obtained by numerous clients. The conditions of tricking, the database possessed by clients who do the deceiving will be not quite the same as the database claimed by different clients. At that point the current database on the client isn't substantial.

III. PROPOSED SYSTEM

This research proposed a database recording system on e-voting using blockchain technology. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process.

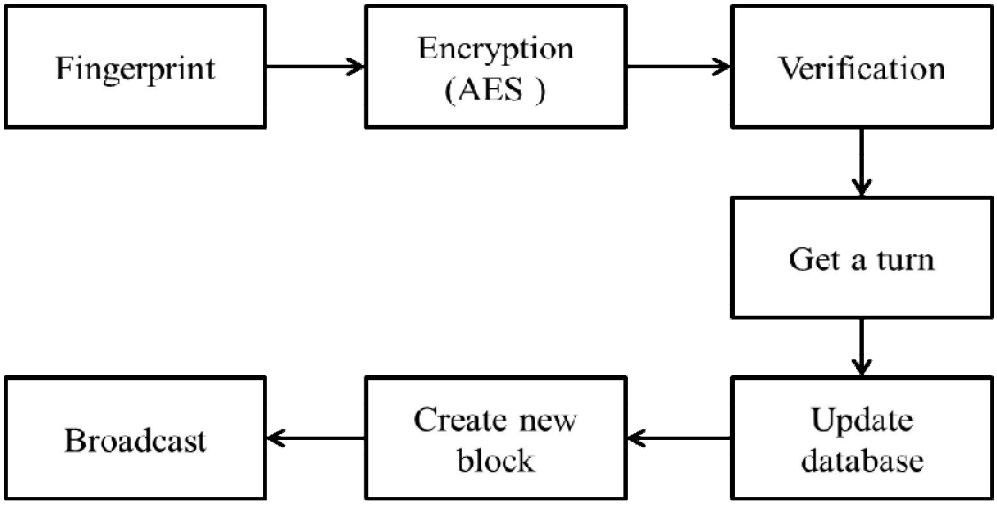

Fig 2.Proposed system

Fingerprint model is used for creating database for person who comes for voting. It is then encrypted using AES algorithm. he more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Further process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then verification is carried out to determine whether the block is valid. Once valid, then the database added with the data in the block.

After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

IV. CONCLUSION

Blockchain technology can be one solution to solve the problems that often occur in the electoral system. The use of hash values in recording 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. The use of the sequence proposed in the blockchain creation process in this system considers that in an electoral system not required for mining as in the Bit coin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation.

REFERRENCES

1. RifaHanifatunnisa Budi RahardjoBlockchain Based E-Voting Recording System Design 978-1-5386-3546-9/17/$31.00 ©2017 IEEE
2. An Exploratory Analysis of Blockchain: Applications, Security, and Related Issues DivyaKamboj T. Andrew Yang Int'l Conf. Scientific Computing | CSC'18 |
3. S. Shah, Q. Kanchwala, and H. Mi, “Block Chain Voting System,” 2016.
4. Christian, “Desain Dan Implementasi Visual Cryptography PadaSistem E-Voting UntukMeningkatkan Anonymity,” InstitutTeknologi Bandung, 2017.
5. S. Nakamoto, “Bitocoin: A Peer-toPeer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2008.
6. J. Bonneau et al, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” in 36th IEEE Symposium on Security and Privacy, May 18-20, 2015.
7. C. Dougherty, “[Vote Chain : Secure Democratic Voting],” 2016.
8. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
9. D. A. Wijaya, Bitcoin Tingkat Lanjut. 2016.
10. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, pp. 577–578, 2016.