EasyChair Preprint

№ 7407

Blockchain Based Online Voting System Using RSA Algorithm

Kingsle Edwin, Hepzibah Christinal and Abraham Chandy

February 1, 2022

BLOCKCHAIN BASED ONLINE VOTING SYSTEM USING RSA ALGORITHM

Kingsle Edwin G, Hepzibah Christinal. A, Abraham Chandy. D

Karunya Institute of Technology and Sciences, Coimbatore, India.

Abstract – Blockchain is a decentralized platform Which provides the security and the integrity of the data that are been saved in the cloud. Electronic polling system provides the voters like accessibility and convenience to the user to solid their state at any time and from any place. Any device which can be connected to the internet can be used to cast their votes from any place in the world. Security for the system is been made sure by using the RSA algorithm.

Despite these advantages, online voting is been approached with caution since it poses new risks. A single flaw can result in a significant shift in vote totals, which can have far-reaching consequences. To address these concerns, blockchain technology was introduced which provides decentralized nodes for electronic voting solution with distributed, non-reputation, and security protection properties. The following article provides an overview of RSA Algorithm based online voting system. The block chain technology was identified to be able to help alleviate some of the challenges in block chain applications, such as privacy protection and transaction speed. The security of remote participation must be realistic for a block chain based electronic voting system to be sustainable, and transaction speed must be addressed for scalability. As a result of these issues. The present framework were found to be in need of improvement to be used in the voting system.

Keywords: blockchain based voting; RSA algorithm; Security; online voting; privacy.

I.INRODUCTION

A poll is a measurement instrument that allows citizen to voice their opinions on a variety of topics, ranging from public policy to public policy affairs and public business, by indicating whether they approve or disapprove. Traditionally, polls were conducted face-to-face, necessitating the presence of the participants. Polls can now be performed remotely thanks to advanced technologies such as the internet, mobile phones and electronic devices. Electronic and

online polls have become increasingly popular in recent years. An inaccurate poll result can occur from a security breach in any area of the system. Which must be prevented or given in a manner comparable to the e-voting system by the polling administration or authority. The similar hazard exists for polls conducted on the public internet. Unauthorized voting, double voting, voter concern, vote buying where a vote buyers offer monetary incentives to vote a certain way or abstain from voting, vote modification where a voting device is either controlled by a malicious programme or a hacker cause unauthorised and potentially undetected changes to a voter's selected vote choices. The effectiveness of such measure is largely decided by the public faith in the electoral process is accurate. When compared to mutual polling, electronic voting improves reliability.

In comparison to traditional voting methods, it has improved the process's efficiency and integrity. Electronic voting procedures, on the other hand, feature a single controller that oversees the whole voting process. Because the central authority's dishonesty, this process leads to selection, which is difficult to correct using conventional procedures. To central authority, the decentralised network might be employed as a contemporary electronic voting technique. For online or electronic voting, block chain technology provides a decentralised node. Because of its end-to-end verification advantages, distributed ledger technologies such as block chain have recently been employed to create electronic voting system. Voting is a new phase of block chain technology, and researchers are attempting to decrease benefits such as transparency, secrecy, and non-repudiation, all of which are necessary for voting applications.

II. OBSTACLE

The process of collecting data and entering the data into the database takes so much of time and also it is an expensive process. There are huge amount of voters and it is very much difficult to collect all the users data and and to process the data and also it requires the huge amount of man power for the process to be done. Even the system is been developed for the use of everyone with a simple and in easy way[1]. The user must do login with their credentials. And it is difficult to track the security and the integrity of the users to overcome this we use the RSA algorithm in this method of block chain based voting system.

III. PROBLEM DEFINITION

All the interaction that the user make with the system is performed remotely through the user's web browser using users electronic devices. This online based voting system is the process of running the elections and surveys online [2]. The user are requested to login through their credentials and the verification is been with the data which is been already stored at the database. Only the user is allowed to proceed when the data is accurate else the session will expire. When the user polls their vote the separate block will be created in the block chain and the hash of the same will be generated. This ensures the security of the votes that are be casted.

IV. BLOCKCHAIN AND RSA

Blockchain is a growing list of blocks. Which contains the hash value of the previous blocks and the time stamp [4]. Each block is been linked using the cryptographic functions. Block chain are basically managed by peer-to-peer network to used as publically with distributed ledger. Where nodes collectively adhere to a protocol to communicate and validate the new blocks [1]. Although the blocks are been unalterable. And block chain is been considered as secure by design. Block chain uses the public key cryptography for the security.

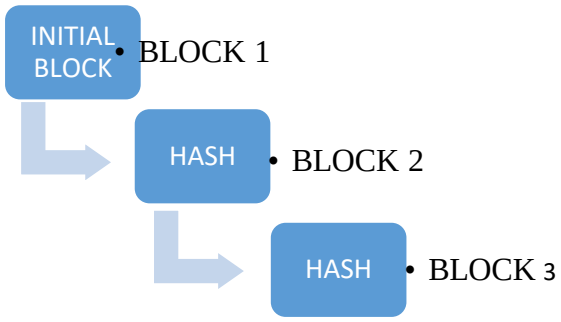

Fig 1 : Hash Connection Of Block

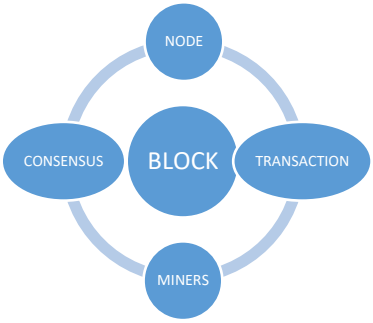

Fig 2 : Block Representation

The RSA algorithm ensure better safeguards of both private and public key. It is also used for the transmission of highly secured data through the unsecure network[3]. Basically RSA consist of four stages key generation, key distribution, encryption, decryption.

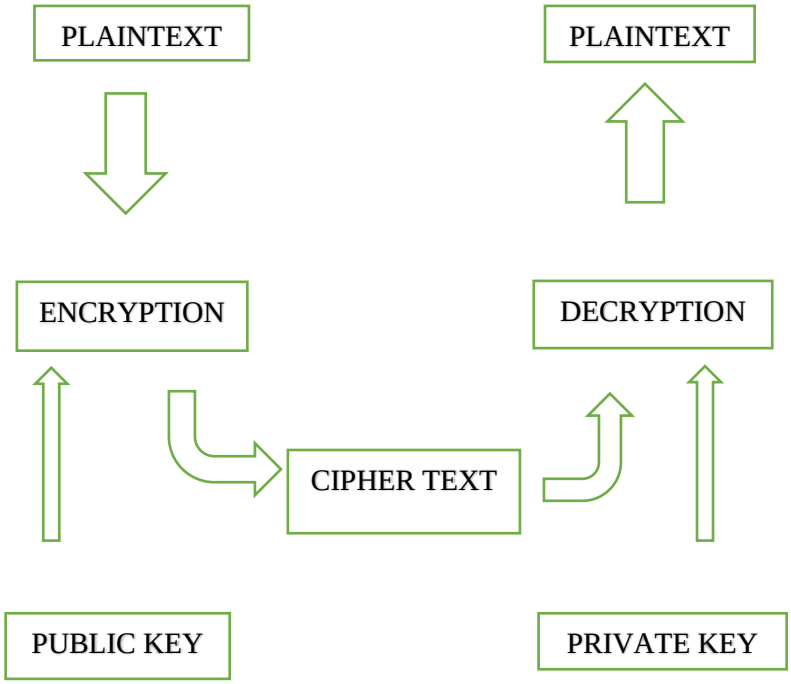

Fig 3 : RSA Technique

It is important to known the role of RSA in Block chain[3]. Public key encryption has become emerging alternative for the conventional cryptographic techniques, How ever blockchain adoption depends a lot on the security, transparency and control. Public key cryptography ensures the effective functioning of security in block chain. It provides 3 major functions

1. Authentication.

2. Integrity Protection.
3. Identity Management.

V. PROPOSED SYSTEM

Electronic voting system is a voting method that uses electronic technology to record nad count votes. Electronic voting is defined as voting enabled by electronic technology and software. Electronic voting is one of the areas where block chain has a huge influence[6]. The stakes are so high that if the computerised voting system is compromised, the ramifications will be enormous. Because a block chain network is decentralized, entirely

The nature of the block chain based network, which is centralised open and consensus-driven ensures that fraud is theoretically impossible until it is properly implemented. The distinct properties of block chain must be considered[5]. There is nothing inherently prohibitive about block chain technology is being used to any other type of crypto money. The concept of using block chain technology to construct a tamper-proof electronic online voting network is gaining popularity. The difference between a block chain based voting system and a regular electronic voting system would be imperceptible to end users.

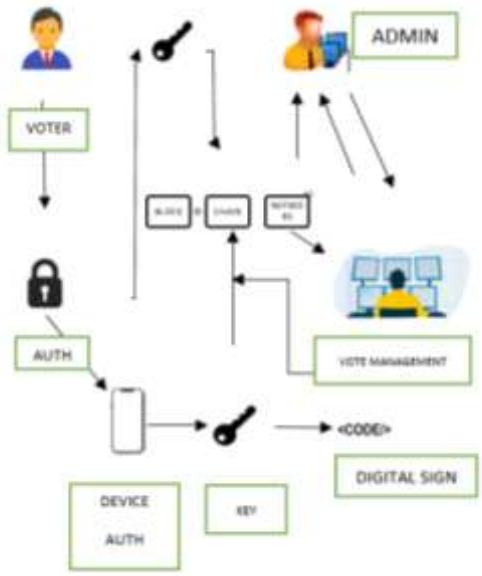

Fig 4 : Working Procedure

Instead of a single server, voting on the block chain will be an encrypted piece of data that is fully open and openly stored on a distributed block chain network[8]. Each encrypted vote is validated by a consensus process on a block chain mechanism, and the public records each vote on distributed copies of the block chain ledger. The government will monitor and record how the votes are been casted and registered, but this information will not be kept private. Despite being decentralised and entirely open, the block chain voting method assures that voters are safeguarded. This means that will block chain electronic voting anyone can count the votes.

Block chain was initially described in 2008 in a novel technique to creating a distributed network. A peer-to-peer network may be built with the use of this innovative technology in which nodes must attain consensus and construct a chain from approved blocks with no need for a central party or trusted controller. Decentralized storage system are one of the most popular implementation of this technology now in use. Clients may safely send their files across a completely decentralise network and avoid the danger of data failure caused by centralised controls by using end-to-end encryption. Storage suppliers must establish their legitimacy in this network[7].

Decentralised storage network are made up of a group of people that are prepared to rent their excess storage space on their computers. Over time the need for more work on the block chain based electronic voting and the comfortable and secure and cost effective than any other network. A smart contract between two parties is also established, detailing the rental length and amount that the consumer must pay for accessing the space

VI. FUTURE WORK

Many concerns with electronic voting may be overcome using block chain technology, making it more cost-effective, comfortable, and secure than any other network. Over time, research has shown particular issues, the need for more work on block chain based electronic voting, and the fact that block chain based electronic voting system are fraught with technical difficulties. The following areas can be worked on in the future,

1. Scalability Overheads.
2. User Identity.
3. Transactional Privacy.
4. Energy Efficiency.
5. Acceptableness.

VII. CONCLUSION

The purpose of this study is to examine and assess current research on electronic voting system based on block chains. The idea of block chain and its applications are introduced first, followed by a discussion of existing electronic voting system. The article addresses recent block chain based electronic voting system research. Block chain, according to several experts might be an excellent match for a decentralised electronic voting system.

Attacks on scalability, a lack of transparency, dependency on untrustworthy systems, and resistance to coercion are all possible disadvantages that must be addressed. We don't know all of the hazards associated with the security and scalability of a block chain based electronic voting system since further study is needed. Adapting block chain based electronic voting system might expose users to security risks and faults they weren't expecting [4].

Block chain technologies necessitate a more complex software design as well as administrative know how. Based on previous experience the above mentioned critical problems should be addressed in more depth during real voting operations. As a consequences, the voting system should be deployed in restricted pilot locations before being expanded. Many security issues in the internet and polling devices still remain. That is why it is critical to recognise that block chain based technology as an electronic voting alternative is still in its infancy.

REFERENCES

1. Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System-Review and Open Research Challenges. Sensors (Basel). 2021 Aug 31;21(17):5874. doi: 10.3390/s21175874. PMID: 34502764; PMCID: PMC8434614.

2. Farley, Naomi, Robert Fitzpatrick and Duncan Jones. "BADGER - Blockchain Auditable Distributed (RSA) key GEneRation." *IACR Cryptol. ePrint Arch.* 2019 (2019): 104.

3. YiHe Liu, Shuang Zhang,Information security and storage of Internet of Things based on block chains,Future Generation Computer Systems,Volume 106,2020,Pages 296-303,ISSN 0167-739X

4. G, Ramya & Perumal, Kumaresan & harshitha, K.. (2020). Online Voting System using Cloud. 1-4. 10.1109/ic-ETITE47903.2020.245.

5. Nazanin Zahed Benisi, Mehdi Aminian, BahmanJavadi,Blockchain-based decentralized storage networks: A survey,Journal of Network and Computer Applications,Volume 162,2020,102656,ISSN 1084-8045
6. Khan, Kashif Mehboob, Junaid Arshad and Muhammad Mubashir Khan. “Secure Digital Voting System Based on Blockchain Technology.” *Int. J. Electron. Gov. Res.* 14 (2018): 53-62.
7. Malkawi, Mohammad & Bani Yassein, Muneer & Bataineh, Asmaa. (2021). Blockchain based voting system for Jordan parliament elections. International Journal of Electrical and Computer Engineering. 11. 4325-4335. 10.11591/ijece.v11i5.pp4325-4335.
8. Leiyong Guo, Hui Xie, Yu Li,Data encryption based blockchain and privacy preserving mechanisms towards big data,Journal of Visual Communication and ImageRepresentation,Volume70,2020,102741,ISSN 1047-3203.