International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06| June2019 www.irjet.net p-ISSN: 2395-0072

Literature survey- Online Voting: Voting System Using Blockchain

Vaibhav Anasune[1], Pradeep Choudhari[2], Madhura Kelapure[3], Pranali Shirke[4] Prasad Halgaonkar[5]

[1,2,3,4]*Student, Department of Computer Engineering, Zeal College of Engineering & Research, Pune, India*[1234]
[5]*Professor, Department of Computer Engineering, Zeal College of Engineering & Research, Pune, India*

Abstract – *Highly advanced security methods are necessary to introduce effective online voting system in the whole world. The aspect of security and transparency is a threat from global election with the conventional system. General elections still use a centralized system where one organization that manages it. Some of the problems that can occur in traditional electoral systems are with an organization that has full control over the database and system, it is possible to manipulate with the database. This paper presents a survey on some previous voting system that is used by different countries and organizations.*

Key Words: e-voting, electronic ballot, homomorphic encryption, centralization

1. INTRODUCTION

The voting system that uses electronic devices to either aid or take care of casting and counting votes is termed as e-voting system. The paper based voting system is replaced by the e-voting. Now a days to decrease the load of man power and delay in result declaration of voting result e-voting system is more in demand by private or public organizations. It also saves papers which are made up of trees which will eventually save the nature disasters.

Since 1960 e-voting systems are being used when the punched card system appeared and was used on seven different counties in US for the presidential election of 1964 and nowadays it has become a very practical way of voting. Electronic voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors.

The e-voting system must guarantee the following Characteristics:

• Eligibility and Authentication: Authorized voters are only able to vote.

• Uniqueness: One voter is allowed to vote to once.

• Accuracy: Voted should be recorded correctly.

• Integrity: Modification or loss of voting data should not be happened that may lead to the failure of system.

• Reliability: System must be designed such that it can be stable even after failures and loss of internet.

• Convenience: Convenient system that will be handled easily with less amount of skillset.

1.1 Electronic Ballot

Electronic voting systems may use electronic ballot to store votes in computer memory. When electronic ballots are used there is no risk of exhausting the supply of ballots. Additionally, these electronic ballots remove the need for printing of paper ballots, a significant cost.

1.2 Cryptographic verification

The concept of election verifiability through cryptographic solutions has emerged in the academic literature to introduce transparency and trust in electronic voting systems. It allows voters and election observers to verify that votes have been recorded, tallied and declared correctly, in a manner independent from the hardware and software running the election.

1.3 Voter intent

Electronic voting machines are able to provide immediate feedback to the voter detecting such possible problems as under voting and over voting which may result in

a spoiled ballot. This immediate feedback can be helpful in successfully determining voter intent.

2. LITERATURE SURVEY

There are lot of practices are made to introduce the variations in electronic and online voting systems where different techniques and methodologies are used. Some of them guarantees the confidentiality and security to the system at some extent, still the voting information and process need to be control and manage with advanced systems that will ensures and guarantees the security and privacy of voter's and voter's information.

2.1 Basic E-voting approach/architecture

The systems that are developed to caste the vote by means of digital approach using online portals and electronic devices use various encryption and decryption techniques to guarantee the secure data transaction.

- **Homomorphic Encryption Technique:**

Homomorphic encryption is a well-known powerful technique with many useful applications. Recently, it has been applied to the design of online voting system.

The voting system based on this encryption uses the exponential ElGamal cryptosystem. Before submission, the contents of each cast ballot are encrypted using the exponential ElGamal encryption. The additive homomorphism property of this crypto system makes it possible to tally encrypted ballots directly without decrypting them.

- **Centralized architecture:**

However, numbers of techniques are present to convert the data in coded format to prevent from manipulation while transferring to the network. One drawback can be discussed here that after the correct data have been stored in the database trust and security is required at substantial level. Centralized storage is inconvenient if the data is esteemed because unauthorized access and attack by hackers will challenge the system in terms of reliability.

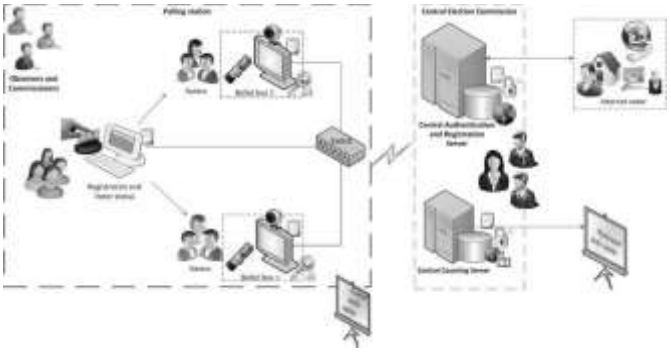

Fig: Centralized Architecture of Voting System

Previous models and architectures are used with help of centralized architecture approach. That may cause ethical and security problem. Collecting the data at a centralized location we take the data at the risk. It can be controlled unfairly. So, fair framework overcomes this problem of storing information to the distributed format with the help of blockchain. Blockchain is distributed ledger that stores all processed transaction in chronological order.

Traditional databases are maintained by a single organization, and that organization has complete control of the database, including the ability to manipulate with the stored data, to censor otherwise valid changes to the data, or to add data fraudulently. For most use cases, this is not a problem since the organization which maintains the database does so for its own benefit, and therefore has no motive to falsify the database's contents; however, there are other use cases, such as a financial network, where the data being stored is too sensitive and the motive to manipulate it is too enticing to allow any single organization to have total control over the database. Even if it could be guaranteed that the responsible organization would never enact a fraudulent change to the database (an assumption which, for many people, is already too much to ask), there is still the possibility that a hacker could break in and manipulate the database to their own ends.

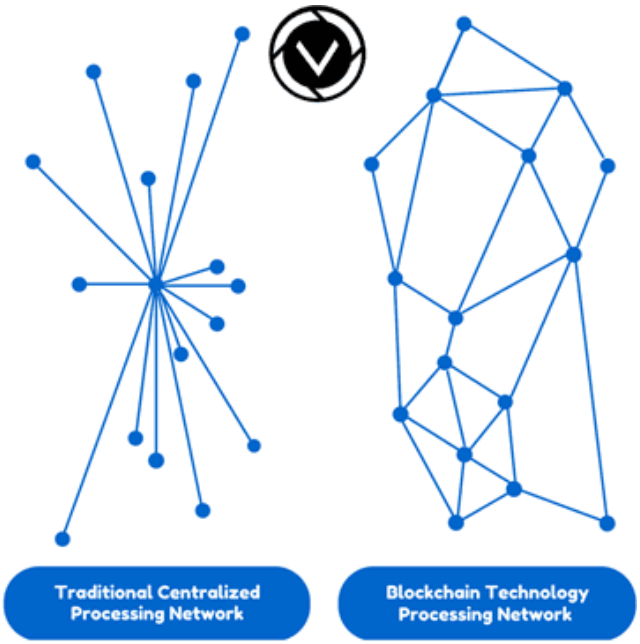

Fig: Centralized and Block Chain Network

Blockchain technology solves these problems by creating a network of computers (called nodes) which each store a copy of the database, and a set of rules (called the consensus protocol) which define the order in which nodes may take turns adding new changes to the database. In this way, all of the nodes agree as to the state of the database at any time, and no one node has the power to falsify the data or to censor changes. The blockchain further requires that an audit trail of all changes to the database is preserved, which allows anyone to audit that the database is correct at any time. This audit trail is composed to the individual changes to the database, which are called transactions. A group of transactions which were all added by a single node on its turn is called a block. Each block contains a reference to the block which preceded it, which establishes an ordering of the blocks. This is the origin of the term "blockchain": it is a chain of blocks, each one containing a link to the previous block and a list of new transactions since that previous block. When a new node joins the network, it starts with an empty database, and downloads all of the blocks, applying the transactions within them to the database, to fast-forward this database to the same state as all the other nodes have. In essence, a blockchain establishes the order in which transactions were applied to the database so that anyone can verify that the database is accurate by rebuilding it from scratch and verifying that at no point was any improper change made.

3. CONCLUSION

In this work, we have seen various techniques and framework used for online voting. This article gives a short review on various methodologies that are used in current online voting. The paper will help to build a system that will face the present and upcoming challenges and will remove drawbacks from these previous architectures.

REFERENCES

1. Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, and Fenglin Han: A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption.

2. Rifa Hanifatunnisa and Budi Rahardjo: Blockchain Based E-Voting Recording System Design

3. Mohammad Hosam Sedky and Essam M. Ramzy Hamed: A Secure e-Government's e-Voting System

4. Himanshu Agarwal and G.N.Pandey: A Secure e-Government's e-Voting System