# Voting System Based on Blockchain Technology

Bhimesh Patil, Darshanesh Naringrekar and Pushpa Mahapatro

April 6, 2022

# VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

Bhimesh Patil
Student,
B.SC.IT,
Vidyalankar School of Information Technology
Vidyalankar College Marg, Wadala (East),
Mumbai - 4000037, India
Email: bhimesh.patil@vsit.edu.in
Tel: +91 75074 21100

Darshanesh Naringrekar
Student,
B.SC.IT,
Vidyalankar School of Information Technology
Vidyalankar College Marg, Wadala (East),
Mumbai - 4000037, India
Email: darshanesh.naringrekar@vsit.edu.in
Tel: +91 90045 88179

**Under the esteemed guidance of**
**Mrs. Pushpa Mahapatro**
**Assistant Professor, Department of Information Technology**

## ABSTRACT

Many people's lives have been aided by digital technology in recent years. Unlike the electoral system, which uses a lot of traditional paper in its implementation. The issue of security and transparency is threatened by the extensive use of the traditional electoral method (offline). General elections are still run under a centralized system, which is overseen by a single institution. Some of the issues that can arise in traditional electoral systems include the ability for an entity with complete control over the database and system to tamper with the database of significant opportunities. Blockchain technology is one of the solutions since it is based on a decentralized system in which multiple people own the entire database. The Bitcoin system, also known as the decentralized Bank system, has used blockchain. One of the main sources of database manipulation can be reduced by using blockchain in the dissemination of datasets on e-voting systems. This study examines the use of the blockchain algorithm to record voting results from every election location. Unlike Bitcoin's Proof of Work, this thesis offered a technique based on each node in the built-in blockchain performing a specified turn on the system.

**Keywords:** Blockchain, Ethereum, smart contracts, electoral system, Bitcoin system, e-voting, security, privacy.

## 1. INTRODUCTION

E-voting is widely used in society life. However, when the decision is financially or politically significant, it is unclear how to assure that the outcome is respected. The most crucial characteristics are always correctness, security, and privacy. Secure e-voting is a type of multi-party computation that is done securely. During the voting process, a group of people make their decisions, which may or may not be kept private. To offer a consistent view to all voters, most e-voting techniques require a trustworthy public bulletin board. The election administrator, on the other hand, has yet to demonstrate that the public message board can be entirely trusted. Because the content is publicly trusted, some people understand blockchain can be used as a bulletin board. As a decentralized database, blockchain offers new tools for developing trustless and decentralized systems. There is no centralized trustworthy coordinator in the blockchain system. Instead, the data block is stored locally by each node in the blockchain system. A decentralized and open-membership peer-to-peer network maintains the blockchain.

## 2. PROBLEM DEFINITION

Initially, this technology was created for the purpose of money transfer. Researchers are attempting to apply Blockchain to other areas of research, such as coordinating the Internet of Things, carbon dating, and healthcare. This sparked the creation of Ethereum, which is widely regarded as a milestone moment in history of blockchain technology. It has a Turing complete programming language and users can realize the function by the smart contract in the Ethereum network.

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

- Eligibility: Only legitimate voters should be able to take part in voting;
- Unreusability: Each voter can vote only once;
- Privacy: No one except the voter can obtain information about the voter’s choice;
- Fairness: No one can obtain intermediate voting results;
- Soundness: Invalid ballots should be detected and not taken into account during tallying;
- Completeness: All valid ballots should be tallied correctly.

## 3. SURVEY OF TECHNOLOGIES

Technology is playing an essential role in providing solutions to worldwide problems. Likewise, it has played its part in Voting Systems. In 2011, a Web-based secure E-voting system with fingerprint authentication was developed, allowing the system administrator to specify the election, party, village headman, polling clerks, and candidate details into the database, as well as set election timings. The village headman is responsible for registering the electors with their fingerprints. Polling clerks can start the election in their authenticated areas. Electors would not be able to vote until the election begins; they will also be validated for voting based on their fingerprint match with previously registered fingerprints in the database, and they will only be able to vote once. The election process can be finished by the system administrator and the election results relevant to the region would be shown after the end of the election process.

In traditional voting systems, the ratio of voters is decreasing day by day therefore in 2015, the idea of an E-Voting System using mobile SMS was proposed named "Mobile-Electronic voting machine (M-EVM) or Modified Electronic voting machine (MEVM)". This system has two different modes. The option for people who do not have mobile phones is an old traditional method, but there is another mode for those who do have mobile phones, which is a requirement for using M-EVM. The voter's name and cellphone number must be registered in the EVM database for M-EVM voting to be successful. Voters can vote for a particular candidate by sending a message in the necessary format, and M-EVM will acknowledge the voter's vote. After voting, that person's name would be removed from the list, and that voter would be unable to vote again. In this system, all registered mobile numbers will be informed about the results of the election after the 1 hour of voting.

## 4. BACKGROUND

The first things that come to mind when thinking about the blockchain are cryptocurrency and smart contracts because of the well-known initiatives in Bitcoin and Ethereum. Bitcoin was the first crypto-currency solution that used a blockchain data structure. Ethereum introduced smart contracts that leverage the power of blockchain immutability and distributed consensus while offering a crypto-currency solution comparable to Bitcoin. The concept of smart contracts was introduced much earlier by Nick Szabo in the 1990s and is described as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". In Ethereum, a smart contract is a piece of code deployed to the network so that everyone has access to it. The result of executing this code is verified by a consensus mechanism and by every member of the network as a whole.

Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts.

Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block in blockchain has a cryptographic hash and timestamp added to the previous block, as shown in Figure 1. A block contains the Merkle tree block header and several transactions. It is a secure networking method that combines computer science and mathematics to hide data and information from others that is called cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms.

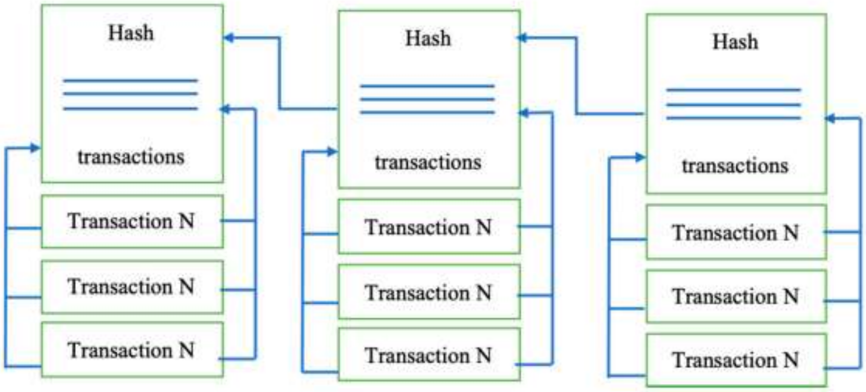

*Figure 1: The Blockchain structure*

As was already mentioned, the blockchain itself is the name for the data structure. All the written data are divided into blocks, and each block contains a hash of all the data from the previous block as part of its data. The aim of using such a data structure is to achieve provable immutability. If a piece of data is changed, the block's hash containing this piece needs to be recalculated, and the hashes of all subsequent blocks also need to be recalculated. It means only the hash of the latest block has to be used to guarantee that all the data remains unchanged. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, which means no one can insert, delete, or alter transactions in an already validated block without it being noticed [24]. The initial zero-block, called the "genesis block," usually contains some network settings, for example, the initial set of validators (those who issue blocks).

### 4.1. Core Components of Blockchain Architecture

These are the main architectural components of Blockchain as shown in Figure 2.

- Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);
- Transaction: It is the blockchain system's smallest building block (records and details), which blockchain uses;
- Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
- Chain: A series of blocks in a particular order;
- Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;
- Consensus: A collection of commands and organizations to carry out blockchain processes.

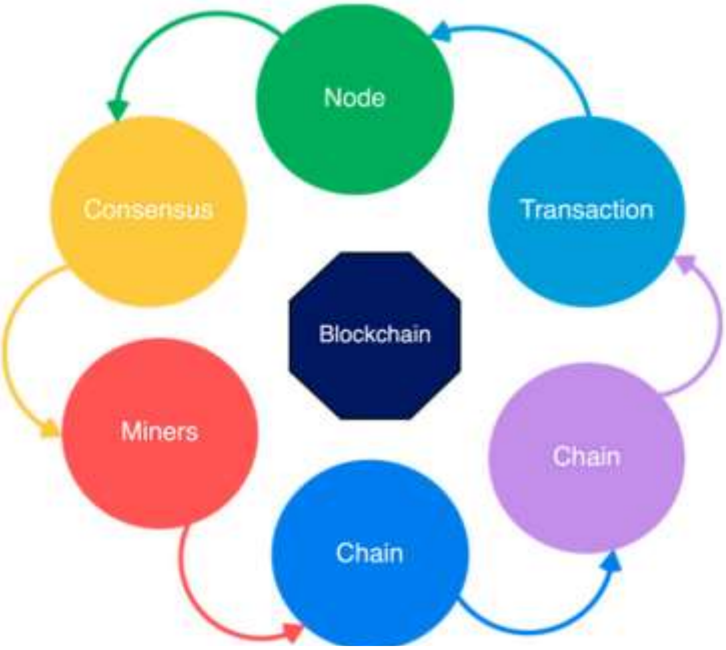

*Figure 2: Core components of blockchain architecture.*

### 4.2. Critical Characteristics of Blockchain Architecture.

Blockchain architecture has many benefits for all sectors that incorporate blockchain. Here are a variety of embedded characteristics as described Figure 3:

- Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved;
- Immutability: Any blockchain documents cannot be changed or deleted;
- Provenance: It refers to the fact that every transaction can be tracked in the blockchain ledger;

- Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process;
- Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system;
- Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network.

Immutability
Anonymity
Cryptography
Provenance
Transparency
Decentralization

*Figure 3: Characteristics of blockchain architecture.*

## 5. How Blockchain Can Transform the Electronic Voting System

Blockchain technology fixed shortcomings in today's method in elections made the polling mechanism clear and accessible, stopped illegal voting, strengthened the data protection, and checked the outcome of the polling. The implementation of the electronic voting method in blockchain is very significant. However, electronic voting carries significant risks such as if an electronic voting system is compromised, all cast votes can probably be manipulated and misused. Electronic voting has thus not yet been adopted on a national scale, considering all its possible advantages. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. In Figure 4, one can see the main difference between both systems. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data. Thus, in this way, one cannot destroy the votes and efficiently verify the votes by tally with other nodes

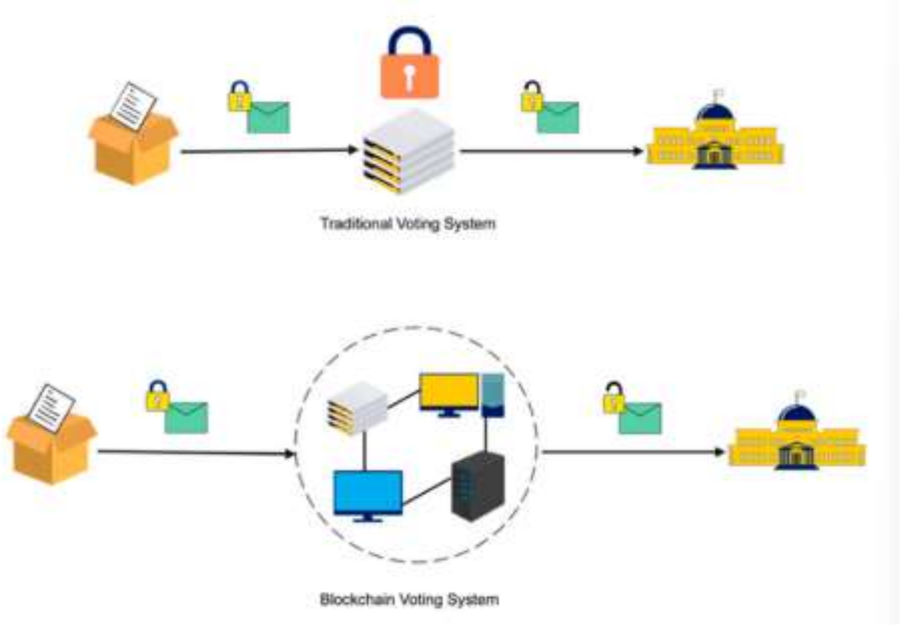

*Figure 4: Traditional vs. blockchain voting system.*

### 1. Security Requirements for Voting System

Suitable electronic voting systems should meet the following electronic voting requirements. Figure 5 shows the main security requirements for electronic voting systems.

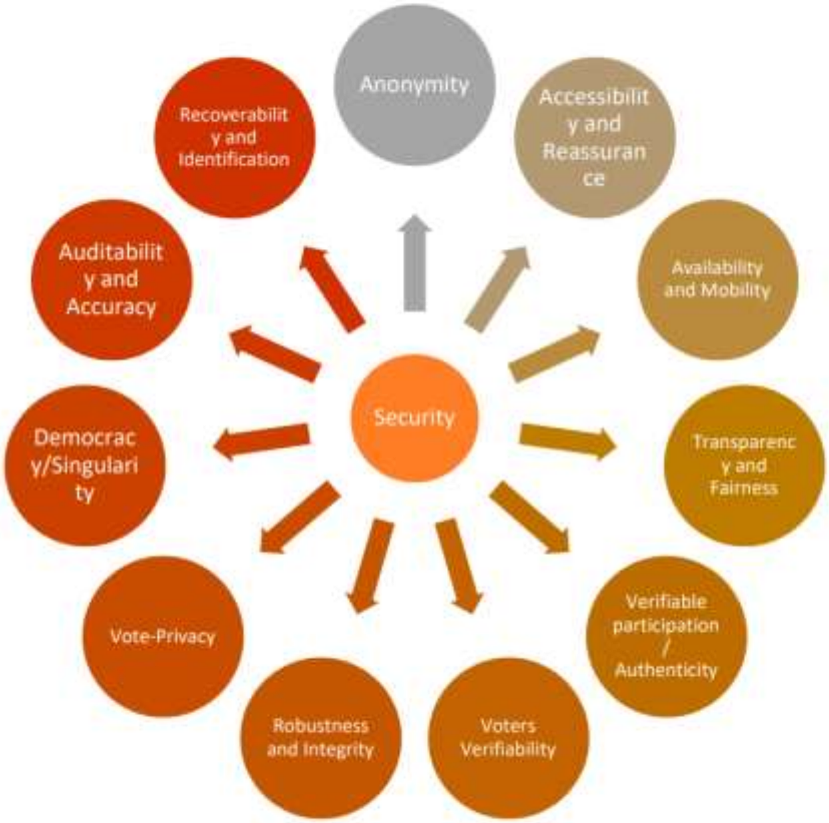
Anonymity
Accessibility and Reassurance
Availability and Mobility
Transparency and Fairness
Verifiable participation / Authenticity
Voters Verifiability
Robustness and Integrity
Vote-Privacy
Democracy/Singularity
Auditability and Accuracy
Recoverability and Identification
Security

*Figure 5: Security requirements for electronic voting system.*

- Anonymity
- Auditability and Accuracy
- Democracy/Singularity
- Vote Privacy
- Robustness and Integrity
- Lack of Evidence
- Transparency and Fairness
- Availability and Mobility
- Verifiable Participation/Authenticity
- Accessibility and Reassurance
- Recoverability and Identification
- Voters Verifiability

## 6. Electronic Voting on Blockchain

This section provides some background information on electronic voting methods. Electronic voting is a voting technique in which votes are recorded or counted using electronic equipment. Electronic voting is usually defined as voting that is supported by some electronic hardware and software. Such regularities should be competent in supporting/implementing various functions, ranging from election setup through vote storage. Kiosks at election offices, laptops, and, more recently, mobile devices are all examples of system types. Voter registration, authentication, voting, and tallying must be incorporated in the electronic voting systems Figure 6.

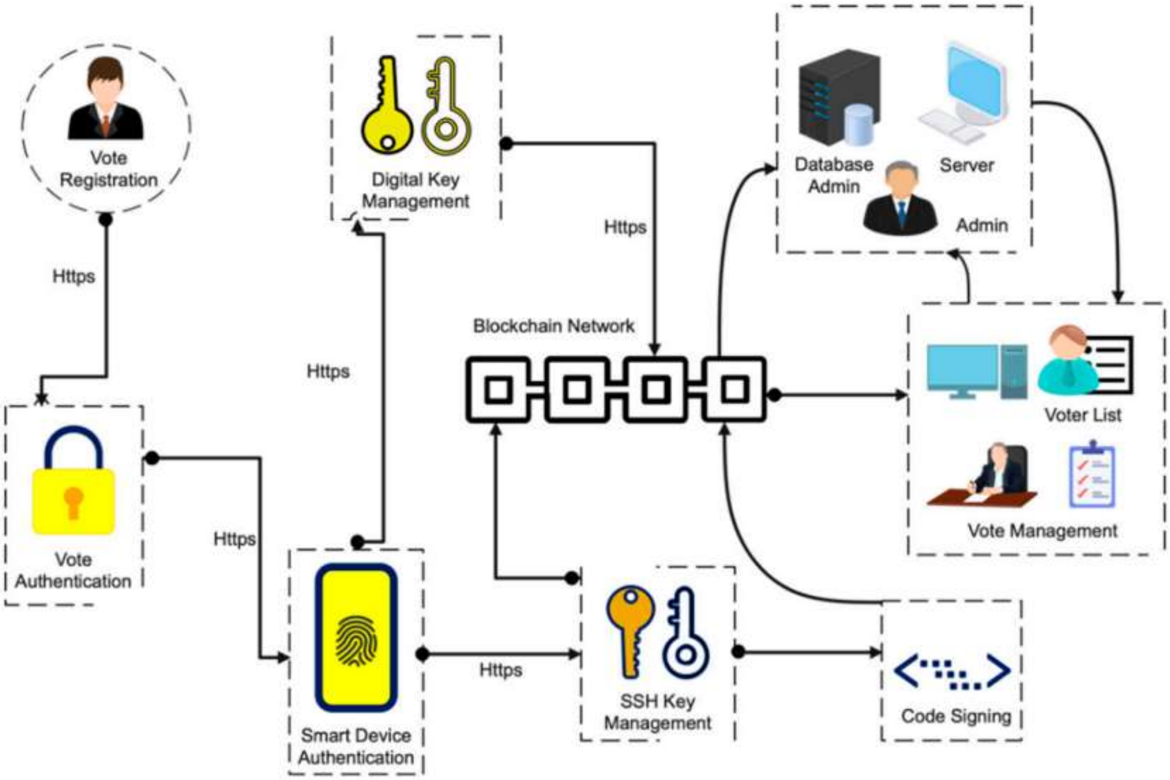

*Figure 6: Blockchain voting systems architectural overview.*

On the other hand, voting on the blockchain will be an encrypted piece of data that is fully open and publicly stored on a distributed blockchain network rather than a single server. A consensus process on a blockchain mechanism validates each encrypted vote, and the public records each vote on distributed copies of the blockchain ledger. The government will observe how votes were cast and recorded, but this information will not be restricted to policy. The blockchain voting system is decentralized and completely open, yet it ensures that voters are protected. This implies that anybody may count the votes with blockchain electronic voting, but no one knows who voted to whom. Standard electronic voting and blockchain-based electronic voting apply to categorically distinct organizational ideas.

## 7. CONCLUSION

The goal of this research is to analyze and evaluate the traditional voting system, as well as the benefits of implementing a blockchain-based E-voting system that makes use of a variety of blockchain-based technologies, as well as a case study of manual voting. Following that, we looked at the differences between the old voting method and the blockchain-based electronic voting system. As a centralized voting mechanism, the implementation employs blockchain. This system will use blockchain as both a network and a database to hold voter information and credentials that will be used for authentication. For the voting process, the system will use the candidate's or voter's information. Furthermore, all voters and impartial observers may see the voting records kept in these suggested systems. On the other hand, researchers discovered that most publications on blockchain-based electronic voting identified and addressed similar issues. There have been many study gaps in electronic voting that need to be addressed in future studies. Scalability attacks, lack of transparency, reliance on untrustworthy systems, and resistance to compulsion are all potential drawbacks that must be addressed. Adopting blockchain voting methods may expose users to unforeseen security risks and flaws. Blockchain technologies require a more sophisticated software architecture as well as managerial expertise. The above-mentioned crucial concerns should be addressed in more depth during actual voting procedures, based on experience.

As a result, electronic voting systems should initially be implemented in limited pilot areas before being expanded. Many security flaws still exist on the internet and polling machines. Electronic voting over a secure and dependable internet will need substantial security improvements. Despite its appearance as an ideal solution, the blockchain system could not wholly address the voting system’s issues due to these flaws. This research revealed that blockchain systems raised difficulties that needed to be addressed and that there are still many technical challenges.

## 8. REFERENCES

1) F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.
2) C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.
3) K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on

Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoTSIU.2019.8777471.

4) Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017, 2017, 1043.
5) Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488. [CrossRef]
6) Racsko, P. Blockchain and Democracy. Soc. Econ. 2019, 41, 353–369. [CrossRef]
7) Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. arXiv 2019, arXiv:1906.11078.
8) The Economist. EIU Democracy Index. 2017. Available online: https://infographics.economist.com/2018/DemocracyIndex/ (accessed on 18 January 2020).
9) Cullen, R.; Houghton, C. Democracy online: An assessment of New Zealand government web sites. Gov. Inf. Q. 2000, 17, 243–267. [CrossRef]
10) De Faveri, C.; Moreira, A.; Araújo, J.; Amaral, V. Towards security modeling of e-voting systems. In Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), Beijing, China, 12–16 September 2016.
11) Xiao S., Wang X.A., Wang W., Wang H. (2020) Survey on Blockchain-Based Electronic Voting. In: Barolli L., Nishino H., Miwa H. (eds) Advances in Intelligent Networking and Collaborative Systems. INCoS 2019. Advances in Intelligent Systems and Computing, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3- 030-29035-1_54
12) Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. IEEE Transactions on Dependable and Secure Computing, 1–1. doi:10.1109/tdsc.2020.2979856
13) K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.
14) Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, Blockchain for Electronic Voting System—Review and Open Research Challenges, Sensors 2021, 21, 5874. https://doi.org/10.3390/s21175874
15) Prof. Mrunal Pathak1 , Amol Suradkar2 , Ajinkya Kadam2 , Akansha Ghodeswar2 , Prashant Parde2, Blockchain Based E-Voting System, Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com) doi : https://doi.org/10.32628/IJSRST2182120