THE
INDIAN
JOURNAL
OF
TECHNICAL
EDUCATION

Decentralized and Secure Voting System using Blockchain Technology

S. S. Kolte
Assistant Professor
AISSMS College of Engineering
Pune, Maharashtra

**Arvind Sudarshan, Chatane Shree
EksambekarYash, Gadkari Gaurav**
Students
AISSMS College of Engineering
Pune, Maharashtra

ABSTRACT

Voting in democratic country is a fundamental right granted to every eligible individual by the constitution. Current e-Voting system used isn't transparent and can be improved in a few aspects. All voting data from Electronic Voting Machines (EVMs) are stored on a central server. This creates a single point of failure which can be exploited and tampered with easily. Such flaws cause mistrust in the electoral process. Blockchain is a shared immutable ledger that facilitates the process of recording transactions in a network. It is an emerging technology whose full potential is yet to be realized. Blockchain became popular in 2009 when bitcoin was introduced and used as an alternative to tangible currency and has evolved since. It is a reliable system that can be used in various critical industrial applications. Blockchain has potential to improve the voting system to contest transparent and fair voting. Using this modern technology, a voting system can be implemented which provides transparency leading to fairness in the system. Furthermore, this will overcome the current system flaw of having a single point of failure caused by storing data in a centralized server. In addition to this, election results can be declared faster compared to the current system which might take a few days. The proposed system in this paper shows implementation of voting using blockchain technology.

KEYWORDS: *Blockchain technology, Ethereum virtual machine, Voting system, Secure voting, Consensus*

INTRODUCTION

The electronic voting system can incorporate blockchain technology to perform a fair election and reduce unfairness. Physical voting systems have a number of issues, just like how computerized voting systems aren't ideal enough to be applied widely. This paper presents an overview of blockchain-based voting systems. The proposed platform will provide a framework for conducting voting operations electronically by utilizing blockchain. For our system, we'll employ a blockchain that can be customized and has consensus algorithms. The chain security algorithm has improved the integration and security of voting transactions.

Blockchain: Blockchain is a distributed ledger technology that links together blocks, or records of transactions, using mathematical cryptography. The distributed aspect of blockchain technology, which renders it immutable and virtually hard to hack, is what makes it so popular.

Distributed Ledger: A ledger is a collection of records that details transactions. A distributed ledger is a data structure that may be used to store transactions and is spread over numerous computers connected to a network. Distributed ledger technology, or DLT, is a method of distributing transaction records to any user connected to the network. A sort of distributed ledger technology is blockchain. As a result, all of its users have access to the data, which promotes transparency and eliminates corruption.

Decentralized Application (dApp): A decentralized application (dApp) is a programme designed to function

on a distributed ledger technology, such as a blockchain. Smart contracts are used by it to operate.

Smart Contract: Computer programmes known as "smart contracts" automatically carry out or regulate actions in accordance with the terms of a contract or other agreement. It is applied to blockchain transactions to impose rules. The essential building blocks of cryptocurrencies and NFTs are thought to be smart contracts.

Consensus: Consensus makes sure that all the various blockchain participants reach a consensus regarding the state of the blockchain. Different blockchain applications employ a variety of consensus mechanisms.

Cryptography: Computer science and mathematical theory are the foundations of cryptography. The purpose of cryptography is to provide means of applying techniques linked to encryption to secure and safeguard data and communications.

Ethereum: The open-source Ethereumblockchain uses the solidity programming language to support smart contracts.

BACKGROUND RELATED WORK

A Framework for Transparency in Voting Systems Using Blockchain Technology [1]

1. The transparent voting mechanism using blockchain technology is explained in this paper. It drastically cuts down on the resources and labor used in the voting process. Voting systems built on the blockchain are resistant to manipulation, unlike traditional voting systems that save votes on a centralized database. Blockchain provides a high level of security that may be trusted more than older technologies.

2. Here, voters must finish the voting management system's verification process. To maintain the integrity of voters, the system's database is integrated with the country's database. A transaction is created for each vote and checked against the voter's National ID before being recorded in the blockchain. The voter uses their vote currency after casting a ballot. Blockchain checks his voting system after casting a ballot against the national

voting IDs. Then, before adding them to the chain, miners examine them to weed out malicious votes.

Using Blockchain Technology in E-Voting Systems: An Empirical Analysis [2]

This study compares and contrasts the performance and security of centralized versus blockchain-based electronic voting systems. Similar interfaces were planned for both systems. The backend design systems were the only thing separating them. With blockchain-based systems, users have to join the network using the private key of their digital wallet as their credentials. If all conditions of the contract are satisfied, a new block is generated, processed, and then added to the blockchain, which serves as the system's database. The centralized system required users to login in with their voter ID. The server processes the votes, which are kept in a database before being automatically counted for each candidate. The results showed that BEVS is a little slower than CEVS. This is because the additional block production and validation procedures on a local private blockchain allow it to process queries more quickly than a public blockchain network. However, the BEVS is more efficient and reliable than the CEVS because it runs through the internal server and has a zero error rate. Even with heavy loads, the BEVS's rate of operation can be impacted. The BEVS is demonstrated to be a more secure electronic voting system with fewer vulnerabilities discovered.

Blockchain technology-based decentralized electronic voting system [3]

1. For improved voting system integrity, this article compares and contrasts decentralized blockchain voting with traditional paper ballots.

2. Data like a voter's name or their votes are saved on a decentralized ledger in the decentralized blockchain system. No outside authority has access to or has the ability to alter this data.

3. The usage of currency ballot papers as a voting method is commonplace globally. Due to the availability of the data at a single resource, this does not, however, guarantee the accuracy of the outcome. Blockchain-based voting systems solve the issue that a centralized voting system has. Here,

using blockchain technology, data is distributed across various servers and locations rather than being kept in a single location. Using a peer-to-peer network, the data is distributed among all of the hardware connected to the blockchain.

4. Before voting begins in the Decentralised E-voting system, candidates must register, and voters' identities must first be confirmed before accounts may be created.within this system. Following voter authentication by an authorized party, blockchain makes sure that voting twice is not permitted

A blockchain-based voting system's architecture [4]

The study recommends BlockVOTE, a voting system built on the Blockchain. It focuses on using consensus handling techniques to uphold the security and dependability of the voting system. The paper discusses the limitations of both conventional ballot-based voting procedures and computerized voting technologies. In the proposed architecture, the study describes the operations of Poll Creation, Voting, and Result Tallying. The system was built by the authors of the research using Hyper Ledger and Ethereum, and the results were compared. Poll creator, contract handler, and voter are the players in the system that will perform tasks relating to poll creation, contract development and deployment, and voting.
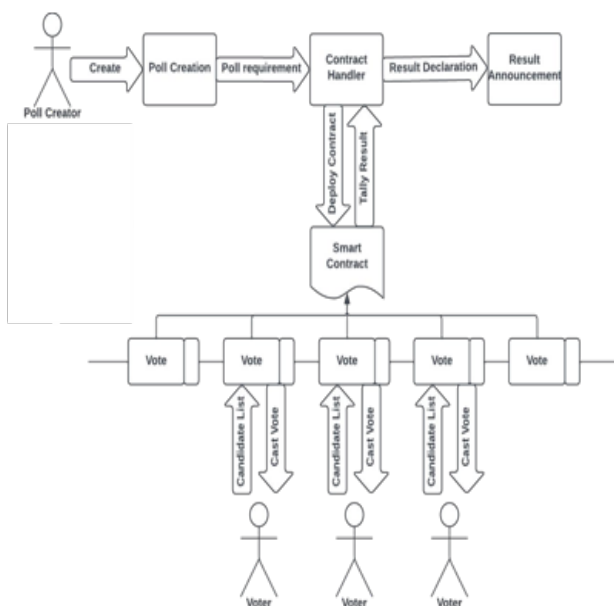

Figure 4. Flow of the System

A Systematic Literature Review of Blockchain Solutions for E-Voting Analysis [5]

In order to understand their particular and make comparisons between them and the traditional voting process, this paper analyses the most recent developments in the blockchain-based electronic voting system. The implementations used, the algorithms used, the techniques used to identify voters and encrypt votes, their resistance to attacks, and other security-related considerations are all taken into consideration while evaluating several blockchain-based e-voting apps in this study. Upon comparison based on the aforementioned traits, various systems' drawbacks and limitations are revealed. Although still in their infancy, voting systems based on blockchain provide an intriguing solution to the shortcomings of traditional voting.

Open Problems and Challenges of a Blockchain-Based E-Voting System [6][7]

1. This study examines and critiques recent research on blockchain-based electronic voting systems. E-voting is the process that uses electronic technologies during an election to facilitate voting and vote counting. Every country has a different electronic voting process which might include electronic voting machines in polling places, central recording of paper votes, and online voting. Centralized calculations are employed in numerous nations. However, in some voting locations, there are also electronic voting machines and internet voting is hardly ever used. Particularly, issues with security and dependability were found when several electronic approaches were tested. Several other aspects of an electronic voting system's security are discussed in this paper, including

- Anonymity: Any association between the registered voters and their identity must remain anonymous.

- Auditability and Accuracy: The outcomes ought to accurately reflect the preferences of the voters.

- Democracy/Singularity: In a democracy/singularity, every eligible person should be able to cast a ballot.. No votes may be cast more than once.

- Vote Privacy: There should be no way for someone to link a particular vote to a specific person.

- Robustness and Integrity: This is evidence that legitimate registered

- voters will easily abstain from voting. Additionally, it inspires others to exercise their right to vote.

- Transparency and Fairness: The results are kept secret from those not directly involved in the counting process until they are released.

- Mobility and Availability: The systems must be accessible at all times during the election.

- Verifiable Participation/Authenticity: If a voter chooses not to cast a ballot, it should be possible for the authorities to determine this.

- Recoverability and Identification: It should be able to locate and retrieve data to avert attacks or data loss.

Fig 2 : System Characteristics

2. The following elements are found in a blockchain:

- Node: It describes a user or computer connected to the blockchain network.

- Transaction: Transactions are the most essential component of a blockchain system since they are the data that is kept in blocks.

- Block: The data structure known as a block is used to store transactional information.

- Chain: A series of transaction blocks arranged in a particular order.

- Miners: Particular nodes that carry out block verification.

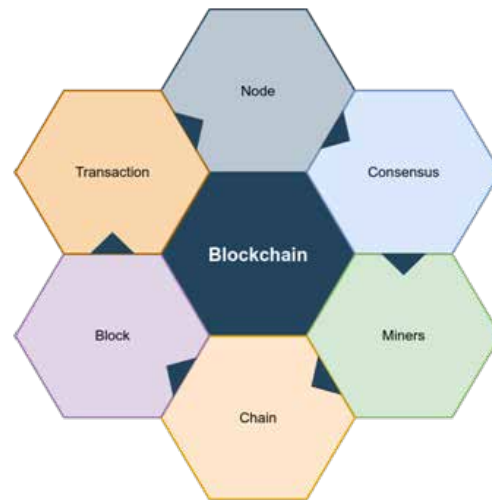- Consensus: An algorithm that determines whether a block should be added into the chain and ensures its validity.

Fig 3 : Elements of System

METHOD

To implement and test a blockchain based voting system, a few components have to be designed. A privately hosted closed blockchain network is required for our contract to run on. This is created using ethereum's Go language based client. To do so, a script is written in JavaScript to automate the following tasks :

1. Ethereum wallet accounts are created for the number of nodes required.

2. On these accounts, the genesis block is initialized.

3. Bootnode is initialized. Bootnode is a node which connects other nodes to each other.

4. Geth (Go Ethereum Client) is run using the accounts created using bootnode initialized in the previous step.

A Solidity based contract is written to execute the application's core functionality. This contract works like the backend for the entire application. This contract is written in solidity version 0.8.19

Decentralized and Secure Voting System using..................   **Kolte, et al**

ElectoralContract {

struct Voter {

    string voterName;

    bool hasVoted;

    bool isLoggedIn;

    string voterPassword;

    address nodeAddress;

uint timestamp;

  }

struct Candidate {

    string candidateName;

    uint256 voteCount;

  }

  // funcaddCandidate : adds candidate for voters to vote

  // funcaddVoter : adds voter

  // funclogin : login functionality for voter

  // funclogout : logout functionality for voter

  // funcgetResult : gets result of elections

  // funcgetCandidates : gets list of candidate names

  // funcgetVotersDetailed : gets all voters information

  // funcvote : cast vote to candidate functionality

};

Algorithm to cast vote :

Require : Voter must have not cast vote earlier

Require : Voter must be logged in

Update :candidate.voteCount++

    // Update vote count for candidate

Update :voter.hasVoted = true

    //Update voting status for voter

Update :voter.timestamp = timestamp

    // Update voting timestamp for voter

Func : logout(voterId)

    // Logout voter
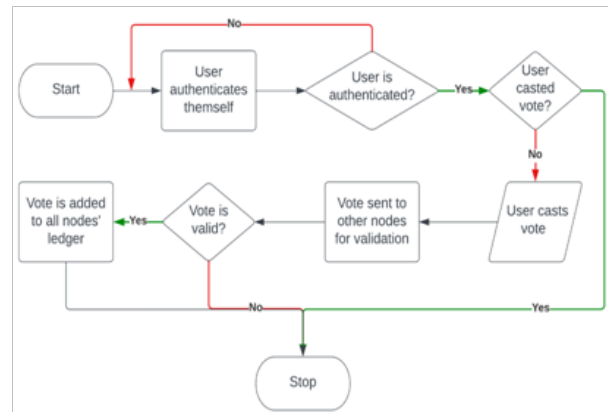
The overall flow followed is :

Figure 4. Flow of the System

Consensus algorithm used in this chain is Proof of Authority (Clique). In PoA consensus, some nodes are given permission to generate new blocks. These nodes are called 'Validators'. PoA leverages the importance of identities. The validators are not staking coins like PoS but rather their own reputation instead.

PoA is suited for private networks such as this one.

Finally, to evaluate the system, some synthetic data is generated and provided to the system and performances tested. To perform this evaluation, python script is written which will perform these tasks :

1. Register a single candidate.
2. Register required number of voters with random names.
3. Login with all voters' credentials.
4. Cast votes by voters with preset probability.
5. Logout all logged in voters.
6. Get result and compile csv.
7. Plot graphs from result

Along with these components, a frontend client is made for a citizen/voter to interact and cast their votes.

Dashboards are also deployed to monitor the network and the data flowing through it.

The system's performance is tested by generating synthetic data which is passed to the system and the time taken for it to process the data and store it in blockchain.

The number of nodes in the system are scaled in range from 1 to 50 while ranging the voters from 10 to 250.

RESULT

Following table shows time taken in seconds by the system to insert data to the private blockchain network and generate results without artificial delay included.

Table 1. Time Taken - (Number Of Nodes Vs Voters)

		Number of nodes									
		1	2	3	4	5	10	15	20	25	50
Voters	10	0.46	7.08	2.4	5.89	20.26	6.27	6.76	10.15	5.94	4.84
	20	0.9	13.56	3.75	5.97	35.4	13.16	17.4	14.87	12.44	56.11
	30	1.33	19.15	6.16	10.16	45.24	81.77	22.4	19.29	19.11	41.7
	40	1.76	8.88	9.25	13.58	61	31.21	30.11	31.57	29.68	33.01
	50	2.3	35.77	11.73	15	65.16	43.83	39.35	37.42	32.23	28.8
	100	4.61	22.82	21.81	30.53	139.74	87.84	71.14	77.71	70.99	111.91
	150	7.93	35.41	34.93	45.02	166.75	100.94	113.08	112.71	111.59	161.79
	200	11.18	49.99	46.33	72.57	0	167.5	143.24	164.77	155	273.67
	250	13.34	152.75	59.7	105.66	0	191.49	169.56	189.36	184.24	209.19

During evaluation of the system, we faced many failures due to block creation taking a long time, blockchain not being synchronized properly across the network, running out of resources for mining and some unexpected system crashes. Due to these crashes, results for 5 nodes, 200 and 250 voters could not be obtained.

CONCLUSION

Through the numerous trial runs and performance testing, we were able to make a few observations. These observations were made based on the performance table in the Result section and self experiences while evaluating the system.

1. As the number of voters increases a gradual increase is observed in time taken to insert transactions and get results.

2. The time taken also increases as the number of nodes in the system is increased. This is due to blockchain synchronization across the network.

3. Less number of nodes showed instability and frequent crashes since load not being distributed well enough. As the nodes increased, the stability increased and less crashes were observed. From the observations, we can say that voting using blockchain technology is feasible and will be beneficial due to its security and distributed nature. Since voting is carried on large scale, it will be stable and solve few issues faced by the current voting system.

REFERENCES

1. Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. IEEE Access, 10, 59959-599

2. Cadiz, J. V., Mariscal, N. A. M., & Ceniza-Canillo, A. M. (2021, December). An empirical analysis of using blockchain technology in e-voting systems. In 2021 1st International Conference in Information and Computing Research (iCORE) (pp. 78-83). IEEE.

3. Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020, October). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) (pp. 176-180). IEEE.

4. Angsuchotmetee, C., Setthawong, P., & Udomviriyalanon, S. (2019, October). Blockvote: An

architecture of a blockchain-based electronic voting system. In 2019 23rd International Computer Science and Engineering Conference (ICSEC) (pp. 110-116). IEEE.

5. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. IEEE Access.

6. Torii, I., Ohtani, K., Shirahama, N., Niwa, T., & Ishii, N. (2012, May). Voice output communication aid application for personal digital assistant for autistic children. In 2012 IEEE/ACIS 11th international Conference on Computer and Information Science (pp. 329-333). IEEE.

7. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17), 5874.

ABOVE AND BEYOND CONVENTIONAL EDUCATION

With the aim of holistic development of students, AISSMS gives an opportunity to learn a lot more than beyond curriculum.
This way we make sure that our students get a head start in their career.

AISSMS GROUP OF INSTITUTES

College of Engineering
Accredited by NAAC 'A+' Grade &
NBA - 6 UG Programs
⊕ *www.aissmscoe.com*

**College of Hotel Management
& Catering Technology**
An Autonomous College Under
Savitribai Phule Pune University
Accredited by NAAC 'A' Grade
⊕ *www.aissmschmct.in*

Polytechnic
NBA Accredited Programmes
⊕ *www.aissmspoly.org.in*

Institute of Information Technology
An Autonomous College Under
Savitribai Phule Pune University
Accredited by NAAC 'A+' Grade
& NBA - 5 UG Programs
⊕ *www.aissmsioit.org*

Institute of Management (MBA)
Accredited by NAAC 'A+' Grade
⊕ *www.aissmsiom.org*

College of Business Administration (CBA)
Approved by Government of Maharashtra
Affiliated to Savitribai Phule Pune University

College of Pharmacy
Accredited by NAAC 'A' Grade
⊕ *www.aissmscop.com*

Private Industrial Training Institute
ISO 9001:2015 certified
⊕ *www.aissmsitcboribhadak.org*

Shri Shivaji Preparatory Military School
Educational Inheritance of Splendid 90 years
⊕ *www.sspms.in*

SSPM Day School & Junior College
50 Glorious Years of Academic Excellence
⊕ *www.sspmdayschool.org*

Placements & Packages (2022-23)

1488	**310**	**49**	**25** LACS	**45** LACS	**1824**	**491**
Total Placements	Between 6 To 9 Lakh - P. A.	Above 9 Lakhs	Hotel Management Highest International Package	Amazon Highest Package-P. A.	No. of Internships	No. of Companies Participated in Drive

Our Accomplishments

- College of Engineering Team QuantumGIS has secured first place in the Smart India Hackathon 2022. Moreover, the college secured All India 5th Rank in E- BAJA All-Terrain Vehicle Competition 2023.

- College of Hotel Management and Catering Technology successfully created a world record by preparing 100 curries in 250 minutes with the help of 250 students & faculty members.

- College of Pharmacy has been reigning champions in the National Pharmacy Week Competition at the undergraduate level, organized by the Indian Pharmaceutical Association, for the past five consecutive years.

- Institute of Management is ranked 10th among affiliated colleges in India by Outlook I-Care Magazine B-School Survey.

- Institute of Information Technology successfully implemented the HAM radio project, ensuring connectivity between remote villages.

For More Details : ☎ **8496045045** ⊕ **www.aissms.org** ✉ **enquiry@aissms.org**