Decentralized and Secure Voting System using Blockchain Technology

Arvind Sudarshan, Chatane Shree Atul, Eksambekar Yash Sagar, Gadkari Gaurav Sudhir

***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**

I. Introduction

To conduct a fair election and lessen unfairness, blockchain technology can be integrated into the electronic voting system. Similar to how computerized voting systems aren't perfect enough to be used on a broad scale, physical voting systems have several problems. An overview of blockchain-based voting systems is provided in this paper. By using blockchain, the proposed platform will offer a framework that can be used to carry out voting operations electronically. We're going to use a customizable blockchain with consensus methods for our system. Voting transactions are more integrated and secure thanks to the chain security algorithm.

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 Ethereum blockchain uses the solidity programming language to support smart contracts.

II. Background and Related Work

A. A Framework to Make Voting System Transparent 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. Compared to earlier technologies, blockchain offers a high level of security that can be trusted more.
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.

B. An Empirical Analysis Of Using Blockchain Technology In E-Voting Systems [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. A new block is created, processed, and then added to the blockchain, which acts as the system's database, if all the terms of the contract are met. Users had to sign in to the centralized system using their voter ID. The votes are tallied automatically for each candidate after being processed by the server and saved in a database. The findings indicated that BEVS is somewhat slower than CEVS. This is because a local private blockchain handles queries more quickly than a public blockchain network due to the additional block production and validation operations. 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. With fewer weaknesses found, the BEVS is also proving to be a more secure electronic voting system.

C. Decentralized E-voting system based on Smart Contract by using Blockchain Technology [3]

1) This Paper Explains the Difference between Ballot paper voting and Blockchain based decentralized casting For better integrity of the voting system.
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. 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.
3) 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.

D. An Architecture of Blockchain based Voting System [4]

The study suggests BlockVOTE, a Blockchain-based voting system. It focuses on employing consensus handling procedures to maintain the voting system's security and dependability. The drawbacks with both traditional ballot-based voting methods and electronic voting systems are discussed in the article. The study defines upon processes Poll Creation, Voting, and Result Tallying in the suggested architecture. The system was constructed by the paper's authors using Ethereum and HyperLedger, and the outcomes were compared. The system will contain the following actors executing duties related to poll creation, contract development and deployment, and voting: poll creator, contract handler, and voter.

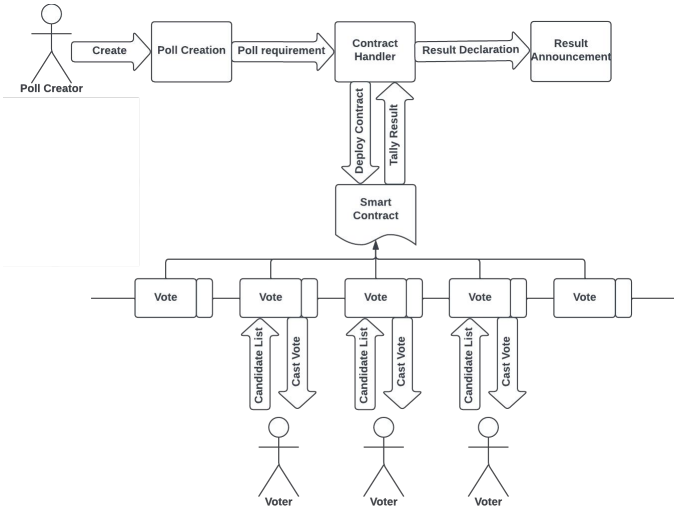

Fig. 1: Blockchain based e-Voting Architecture

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

This study examines the most recent advancements in the blockchain-based electronic voting system to comprehend their specifics and contrasts them with each other and the conventional voting process. Here, various blockchain-based e-voting apps are evaluated based on a variety of factors, including the implementations utilized, the algorithms employed, the methods used to identify voters and encrypt votes, their resilience to assaults, and other security-related factors. After comparing these based on the aforementioned characteristics, these systems' shortcomings and restrictions. Even though the blockchain-based voting systems are still in their infancy, they present an intriguing alternative to the drawbacks of conventional voting.

F. Blockchain Based E-Voting System: Open Issues and Challenges [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
    a) Anonymity: Any association between the registered voters and their identity must remain anonymous.

b) Auditability and Accuracy: The outcomes ought to accurately reflect the preferences of the voters.
c) Democracy/Singularity: Every eligible person should be able to cast a ballot in a democracy/singularity. No votes may be cast more than once.
d) Vote Privacy: No one should be able to connect a specific vote to a specific person.
e) 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.
f) Transparency and Fairness: The results are kept secret from those not directly involved in the counting process until they are released.
g) Availability and Mobility: The systems must be accessible at all times during the election.
h) Verifiable Participation/Authenticity: If a voter chooses not to cast a ballot, it should be possible for the authorities to determine this.
i) Recoverability and Identification: To prevent attacks or data losses, it should be able to track down and retrieve data.

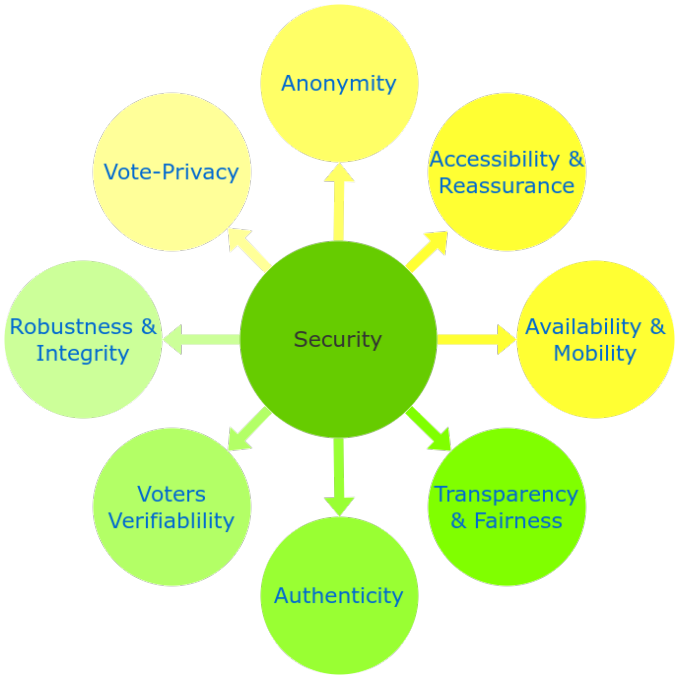

Fig. 2: Security Requirements for Electronic Voting System

2) The following elements are found in a blockchain:
   a) Node: It describes a user or computer connected to the blockchain network.
   b) Transaction: Transactions are the most essential component of a blockchain system since they are the data that is kept in blocks.
   c) Block: The data structure known as a block is used to store transactional information.
   d) Chain: A series of transaction blocks arranged in a particular order.
   e) Miners: Particular nodes that carry out block verification.
   f) Consensus: An algorithm that determines whether a block should be added into the chain and ensures its validity.

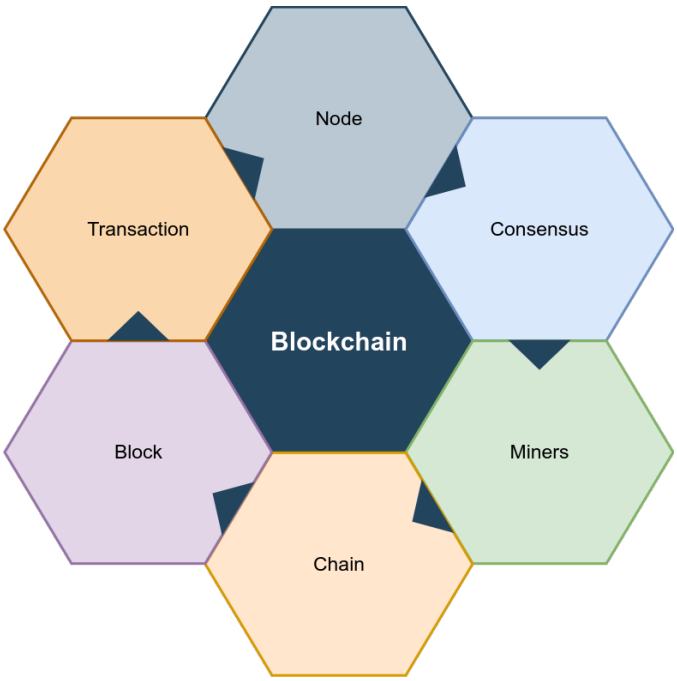

Fig. 3: Core Components of Blockchain Architecture

III. Methodology

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 :

```
ElectoralContract {

        struct Voter {
                string voterName;
                bool hasVoted;
                bool isLoggedIn;
                string voterPassword;
                address nodeAddress;
                uint timestamp;
        }

        struct Candidate {
                string candidateName;
                uint256 voteCount;
        }

        // func addCandidate : adds candidate for voters to vote
        // func addVoter : adds voter
        // func login : login functionality for voter
        // func logout : logout functionality for voter
        // func getResult : gets result of elections
        // func getCandidates : gets list of candidate names
        // func getVotersDetailed : gets all voters information
        // func vote : 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 :

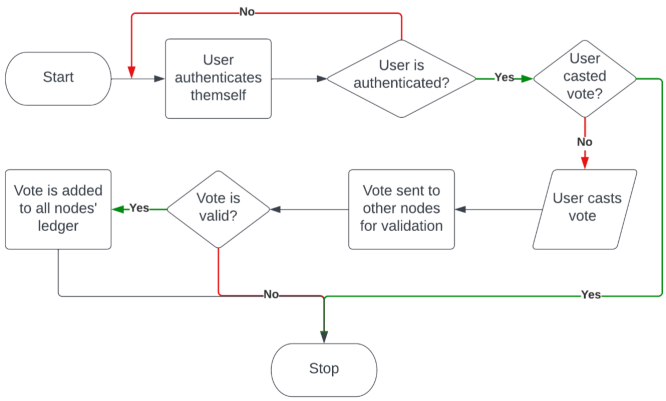

Fig. 4: Flow of the system

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 results.

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.

IV. Results

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

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.

V. 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

TABLE I: 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	-	167.5	143.24	164.77	155	273.67
	250	13.34	152.75	59.7	105.66	-	191.49	169.56	189.36	184.24	209.19

on large scales, it will be stable and solve few issues faced by the current voting system.

REFERENCES

[1] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59959–59969, 2022.

[2] J. V. Cadiz, N. A. M. Mariscal, and A. M. Ceniza-Canillo, "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, 2021.

[3] A. M. Al-Madani, A. T. Gaikwad, V. Mahale, and Z. A. Ahmed, "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, 2020.

[4] C. Angsuchotmetee, P. Setthawong, and S. Udomviriyalanon, "Blockvote: An architecture of a blockchain-based electronic voting system," in *2019 23rd International Computer Science and Engineering Conference (ICSEC)*, pp. 110–116, IEEE, 2019.

[5] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: A systematic literature review," *IEEE Access*, 2022.

[6] Z. Khudoykulov, U. Tojiakbarova, S. Bozorov, and D. Ourbonalieva, "Blockchain based e-voting system: Open issues and challenges," in *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–5, IEEE, 2021.

[7] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.