Survey on Blockchain Technology and its application in Electoral Voting System

Arvind Sudarshan[1], Chatane Shree Atul[2], Eksambekar Yash Sagar[3], Gadkari Gaurav Sudhir[4], Snehal S. Kolte[5]

[1, 2, 3, 4, 5]*Computer Department, AISSMS College of Engineering, Savitribai Phule Pune University*

***Abstract*— Blockchain technology can be used in the E-voting system to conduct a fair election and reduce injustice. The physical voting systems have many flaws in it as well as the digital voting systems are not perfect enough to be implemented on a large scale. This paper presents an overview of Blockchain based voting systems. The proposed platform will provide a framework that can be implemented to conduct voting activity digitally through blockchain. Our proposed system will use a flexible blockchain with consensus algorithms. The Chain security algorithm used in makes voting transactions more secure and integrated.**

***Keywords*— E-polling, Voting System, Blockchain Application, Blockchain Voting, E-voting, Electoral System, Blockchain, Cryptographic Hash, Secure Voting**

I. INTRODUCTION

This paper contains Literature survey and its outcomes conducted for implementing a Decentralized Application which uses Blockchain Technology for Electronic Voting System in general elections. The survey covered basics of blockchain, types of blockchains, various consensus algorithms included in blockchain technology, its scalability, existing solutions with their advantages and disadvantages, architectures and frameworks in past.

As a part of this survey, we studied existing electoral voting systems: traditional ballot paper and e-Voting. On doing so we understood certain flaws and disadvantages which could be overcome by combining existing system with new and trending Blockchain technology.

Blockchain: Blockchain is like a distributed ledger technology consisting records of transactions called as blocks that are linked together using mathematical cryptography. Blockchain technology is popular because of its distributed nature which makes it immutable and practically impossible to hack.

Distributed Ledger: Ledger is a records collection containing information about transactions. Distributed ledger is a data structure capable of storing said transactions which is distributed across different computers on the network. DLT (Distributed Ledger Technology) is technology that distributes transaction records to all the users participating in network. Blockchain is a type of Distributed Ledger Technology(DLT). Hence the data is shared among all its users providing transparency and preventing corruption.

Decentralized Application(dApp): dApp is an application built to run on decentralized computing, blockchain or any other distributed ledger system. It makes use of smart contracts for its functioning.

Smart Contract: Smart contracts are computer programs that automatically execute or control actions according to the terms of a contract or an agreement. It is used to enforce rules in blockchain transaction. Smart contracts are considered fundamental building blocks for cryptocurrencies and NFTs.

Consensus: Consensus ensures that all the different users participating in blockchain come to a mutual agreement regarding the state of blockchain. There are numerous consensus mechanisms that are used by different blockchain applications.

Cryptography: Cryptography is based on mathematical theory and computer science. Cryptography's importance is to provide methods to secure and protect dat and communications using encryption related techniques.

Ethereum: Ethereum is an open-source blockchain which provides smart contract functionality using solidity programming language.

II. LITERATURE SURVEY

A. *Emergence of Blockchain [1]*

Blockchain gained most of its fame from bitcoin, a cryptocurrency.

It is the backbone of bitcoin.The concept of blockchain was introduced in 2008 and implemented a year later. Satoshi Nakamoto is dubbed as the creator of blockchain.Blockchain has several different characteristics like decentralisation, persistence, anonymity and auditability. Blockchain has various diverse applications other than bitcoin.Its ability to conduct transactions without banks make it a strong contender for online payments.

B. *Brief information on evolution and versions of Blockchain Technology [2]*

This paper covers the Blockchain technology's evolution, its security and architecture.

Blockchain 1.0 is used in bitcoin founded by anonymous person with pseudoname Satoshi Nakamoto. Cryptocurrencies are the first applications of Blockchain technology and are already functional as a digital payment alternative on the World Wide Web.

Blockchain 2.0 is based on Smart Contracts. It is used for transferring assets like bonds, stocks, loans, Properties etc. Afterwards it is realised that that Blockchain can revolutionise for all the industries.

Blockchain 3.0 provides a platform for development of secure applications for all the industries rather than only money exchange.It supports large scale interconnection using web technology.

C. *Characteristics of Blockchain [3]*

- **Cost effective:** In traditional systems there is a need of some central organizaion to verify the validity of transactions. Blockchain is a peer to peer network(P2P). The absence of a central agency reduces the cost per transaction.
- **Persistence:** Blockchain has one important property of persistence, Each block has the ability to maintain its records. This helps in keeping the data tamper proof.
- **Validity:** The execution is not carried out every time. This system has three roles, proposer, acceptor, learner.
- **Anonymity & Identity:** The centralised systems require to know you as a person. You need to register your identity proof with those authorities. Whereas with blockchain, the user data remains fairly anonymous.
- **Auditability:** The block added to the blockchain remains there forever. This helps in checking transaction history. In private blockchain the auditability is least and depends on the central entity. In permissioned blockchain there is a little bit of auditability. In public blockchain have the most auditability.

D. *Blockchain types and their comparision [4]*

In Blockchain Technology, there exists three major types: Privete, Consortium and Public blockchain. Since a network will have to be created, a comparison must be made on what kind of network must be used for the same. The types are compared on the basis of Consensus determination, Read permission, Immutability, Efficiency, whether it is centralised or not and the Consensus process. Depending upon the application, a developer must decide what kind of blockchain should be used. Table I shows a comparision between the types of blockchains.

TABLE I
Types of Blockchains

Property	**Types of Blockchain**		
	Private	**Consortium**	**Public**
Consensus determination	Single Organisation	Selected nodes	All participating miners
Read permission	Could be public or restricted	Could be public or restricted	Public
Immutability	Could be tampered	Could be tampered	Nearly impossible to tamper
Efficiency	High	High	Low
Centralised	Yes	Partial	No
Consensus process	Permissioned	Permissioned	Permissionless

E. *Consensus algorithms used in Blockchain Technology [5]*

The Oxford Dictionary meaning of word consensus is: an opinion that all members of a group agree with. In Blockchain Technology every transaction must be verified and agreed upon by validators in the network before being inserted. To do so, various consensus algorithms have been defined for use. Few of the most used consensus algorithms are Proof of Stake (PoS) algorithm and Proof of Work (PoW) algorithm.

In this paper referenced, the authors have mentioned a few of the consensus algorithms used and their comparative analysis. Some High-profile consensus algorithms mentioned in the paper are Proof of Work (PoW), Proof of Stake (PoS), Proof of Importance (PoI), Delegated Proof of Stake (dPOS), Stellar Consensus Protocol (SCP) and Ripple Protocol Consensus Algorithm (RPCA). The authors have compared these algorithms on the basis of Security, Scalability and Power Consumption. A consensus algorithm characteristic comparison is provided in Table II.

TABLE II
Consensus Algorithm Comparision

Property	Algorithm Name					
	PoW	RPCA	PoS	SCP	dPOS	PoI
Energy Saving	No	Yes	Partial	Yes	Partial	Yes
Tolerated power of adversary	<25% computing power	<20% faulty nodes	<51% stake	Variable	<51% validators	<50% importance
Example	Bitcoin	Ripple	Cardano	Stellar	EOS	NEM

F. *Scalability of Blockchain [6]*

- **Bitcoin-Cash:** It is another form of cryptocurrency. It is the hard fork from bitcoin's codebase. The main idea is to solve the scalability issue of the blockchain. The solution here is to increase the block size while keeping the block interval the same. The block size of bitcoin was 1 MB, but now bitcoin and bitcoin cash has increased its blocksize to 8 MB. After that there was further increase in the block size of bitcoin cash to 32 MB.However we cannot increase the blocksize infinitely as there is a limitation to the intra-blockchain bandwidth. The larger block sizes may also lead to the problems of centralization.
- **Block compression:** In compact block relay technique the data structure is little altered. The block contains the headers and some short transaction IDs, used to match transactions already available to the receivers. The compact block messages are sent and receivers process these messages. The node A sends the compact block to the node B. When node B receives the compact block it calculates the transaction IDs in the memory pool and matches it with the transactions IDs in the compact block. If all transactions are available the block is reconstructed if not node B sends the getblocktxn message to node A to receive all transaction data. After that the block is constructed. In low bandwidth relaying the compact blocks are sent only if the request is made.

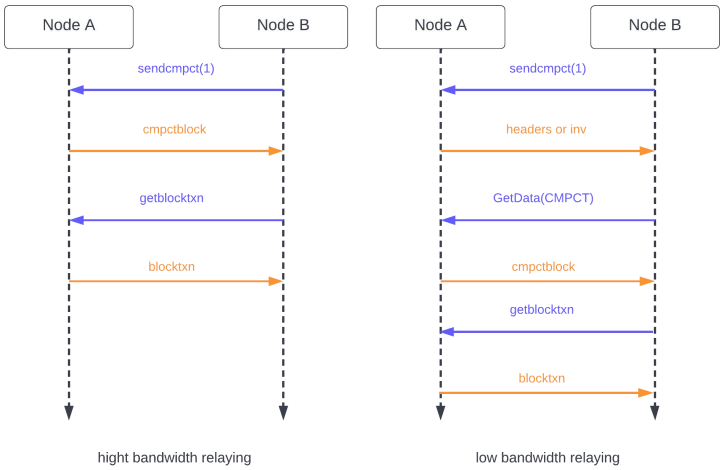

Fig. 1 Block compression

- **Storage scheme Optimization:** This scheme has a consensus unit. It has a number of nodes in it. The blocks of the whole chain are assigned to a single unit. This reduces the total query cost. Jidar is another approach. The main idea is to store only relevant data they are interested in. Small part of the data is stored including the relevant transactions and the merkel branch. If at all we need all the block data, the nodes ask the other nodes and the complete blocks are constructed out of it. There needs to be some incentives for other blocks to help the block asking for the complete data.

G. *An Empirical Analysis Of Using Blockchain Technology In E-Voting Systems [7]*

This paper discusses the difference between a centralised e-voting system and a blockchain based e-voting system in terms of performance and security. Both systems were designed to have similar interfaces. The only difference between them was the systems used to design the backend. With blockchain based systems, the users needed to use their digital wallet's private key as their credentials to connect to the network. If all the conditions of the contact are satisfied, a new

block is created, processed and then added to the blockchain, which serves as the database for this system. The centralised system required users to log in with their voter ID. The votes are processed by the server and stored in a database, which automatically counts the number of votes for each candidate. Results showed that BEVS is slightly slower than CEVS. This is due to the additional processes of block validation and creation while using a local private blockchain, it processes requests faster than a public blockchain network. However, the BEVS is more reliable when it comes to efficiency as it has a zero error rate compared to the CEVS with its errors. through the internal server. However, the rate at which the BEVS works can be affected even by heavy loads. The BEVS is also proving to be a more secure electronic voting system with fewer identified vulnerabilities.

H. *A Framework to Make Voting System Transparent Using Blockchain Technology [8]*

This paper explains about the transparent voting system using blockchain technology. It reduces a lot of resources and efforts in the polling system. Unlike the traditional voting system which stores votes on a centralised system, blockchain based voting systems are not easily tampered. Blockchain provides a high level of security that can be trusted more than the previously used technologies.

Here voters need to complete verification into the voting management system. The nation's database is integrated with the system's database to keep voters' integrity. For every vote, a transaction is generated against the voter's National ID then the transaction is saved in blockchain. After casting a vote his/her vote coin is used. After casting vote blockchain verifies his voting system by comparing with the national voting ids. Then miners analyse them to remove malicious votes before adding them to the chain.

I. *Decentralised E-voting system based on Smart Contract by using Blockchain Technology [9]*

This Paper Explains the Difference between Ballot paper voting and Blockchain based decentralised casting For better integrity of the voting system.

Here in Decentralised Blockchain System data like the name of voter or votes is saved on a decentralised ledger. This data neither be accessed nor be changed by any third party authority. Currency ballot paper is a widely used voting system worldwide. But this doesn't guarantee the correctness of the result Due to availability of data at a single resource. This problem is faced by a centralised voting system and is solved by Blockchain based voting systems. Here in Blockchain Technology the data is not stored on a central location but is allotted in different locations on different servers. The data which is distributed across each device connected to the blockchain using a peer-to-peer system.

In the Decentralised E-voting system candidate registration is done before the voting process starts and then voters identity is verified before the creating account.In this system. The authorised person authenticates the voter and then blockchain ensures the double voting is not allowed.

J. *An Architecture of Blockchain based Voting System [10]*

The paper proposes a Blockchain-based voting system called BlockVOTE. It focuses on keeping the voting system secure and trustable using consensus handling mechanisms. The paper covers Traditional Ballot based Voting systems and Electronic based Voting Systems with both their issues. In the proposed architecture, the paper defines upon processes Poll Creation, Voting and Result Tallying. Authors of the paper implemented the system using Ethereum and HyperLedger and compared the results. The system will have the following actors: Poll Creator, Contract Handler and Voter performing tasks of Poll Creation, Contract creation and deployment and Voting.

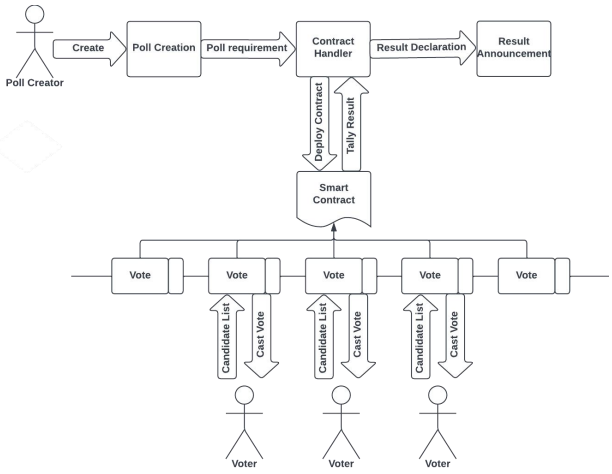

Fig. 2 Blockchain based e-Voting Architecture

K. *Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review [11]*

This paper reviews the latest innovations in the blockchain based e-voting system to understand their particulars and compares them with each other as well as the traditional voting process. Various blockchain based e-voting applications here are being compared based on many parameters like implementations used, algorithms used, voter identification methods, vote encryption methods, how they fare against attacks and their security properties. After comparing these based on the said factors, limitations and constraints of these systems. Even though the blockchain based systems for voting may be in their initial phases, they offer an interesting solution to the problems of traditional voting.

L. *Blockchain Based E-Voting System: Open Issues and Challenges [12][13]*

This paper analyses current research on blockchain electronic voting systems and identifies issues in it. E-Voting defines the process that uses electronic tools in the process of elections for voting and counting purposes. The procedure for electronic voting varies from country to country. which may include voting machines on polling stations, centralised accounting of paper bills and voting on the Internet. In many countries, centralised calculations are used. Sometimes, however, they also use electronic voting machines in places of voting. However, the use of the internet is minimal. In particular, electronic approaches have been tested in several places and problems with security and reliability were noted. This paper also talks about several factors that makes an e-voting system secure like,

i. **Anonymity:** Any correlation between registered voters and voter identities shall be anonymous.
ii. **Auditability and Accuracy:** The results should be accurate and should precisely correspond to the voter sentiment.
iii. **Democracy/Singularity:** Every eligible person should be able to vote. There shall be no duplication of votes.
iv. **Vote Privacy:** No one should be able to associate a particular vote to an individual.
v. **Robustness and Integrity:** It is the proof that registered voters will abstain without problems. It also encourages others to cast their legitimate votes.
vi. **Transparency and Fairness:** No one outside the people involved with the counting process can find out about the results before they are announced.
vii. **Availability and Mobility:** The systems should always be available during the electoral process.
viii. **Verifiable Participation/Authenticity:** The authorities should be able to check if someone abstained from voting.
ix. **Recoverability and Identification:** It should be able to track and restore data in order to avoid attacks or data losses.

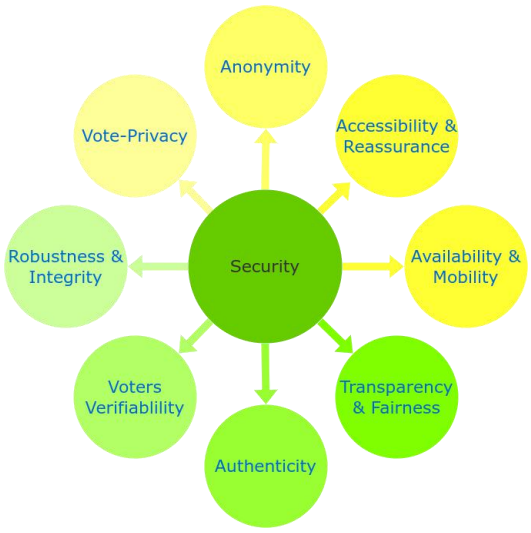

Fig. 3 Security Requirements for electronic voting system

A blockchain includes the following components:

i. **Node:** It refers computer or user participating in the blockchain network.
ii. **Transaction:** The is the data stored in blocks making it the most fundamental part of a blockchain system.
iii. **Block:** It is the data structure which is used for storing the transaction information.
iv. **Chain:** A sequence of blocks which are organized in some specific order.
v. **Miners:** Specific nodes which perform the block verification process.
vi. **Consensus:** Algorithm which ensures validity of block and decides whether it should be inserted to chain or not.

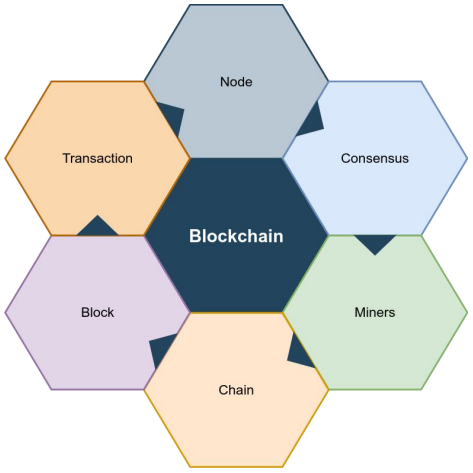

Fig. 4 Core Components of Blockchain Architecture

III. Outcome of Literature Survey

Blockchain is a new emerging technology. It is currently under research to implement with perfection. Blockchain has shown some promising applications. Some of its famous applications include finance industry, healthcare industry, art industry etc. The concept of blockchain was proposed in 2008 by a person named Satoshi Nakamoto and was actualized a year later. Based on the application of the blockchain there are different characteristics of it that make it different. They are cost effective. Reduces the overall cost of conducting transactions on our case voting. There is no need for a central agency. Persistence helps us keep track of all the logs of voting in the system. There are three roles in the blocks. The one who proposes a transaction/vote. The one who checks or validates whether the votes are valid or not and applies it to itself. And lastly the one who learns from all these transactions and implements the votes to itself. Blockchain systems provides you with anonymity over traditional systems. They do not collect the users private data. The blocks added to the system remain there forever. This facilitates auditing of the transaction or in our cases votes. There are different tradeoffs to make blockchain scalable. Lately there was a fork made to bitcoin to increase its scalability. Bitcoin having a block size of 1MB could accommodate a smaller number of transactions, whereas the fork (now known as bitcoin-cash) has a block size of 8-32 MB. This increases the number of transactions that can be accommodated in a block. Another technique to increase scalability is to tweak the data structure of the block. It calculates the transaction IDs in the memory pool and matches it with the transaction IDs in the compact block.

Advantages

1. The votes cannot be manipulated as consensus algorithms are used.
2. Before a node (i.e a vote) is added to the chain, its legitimacy is verified by various nodes in the network.
3. Every node in the network has a copy of the ledger and therefore the transparency of the process increases.
4. There is no central server/system which reduces the possibility of data loss and malicious attacks.
5. Also since there is no central server/system it increases the reliability of the system as there is no single point of failure.
6. The counting process also becomes more efficient and use of blockchain increases the accuracy of the system.
7. Mechanisms can be put in place to prevent duplicate voting.

Disadvantages

1. As the number of nodes increases, the amount of time required to process a transaction also increases.
2. There is a chance that the voters can be intimidated or coerced to vote against their will.
3. There needs to be proper power supply and backup in order for the system to function seamlessly.
4. As blockchain is resource intensive the cost of hardware increases and power consumption increases.
5. If the number of active nodes decrease then the security of the blockchain aso decreases.

6. People in general are reluctant to use new technology.
7. As the number of nodes increases, it becomes increasingly difficult to maintain the nodes.

IV. Conclusion

As we have seen, all the above-mentioned papers have their own advantages. By evaluating all the advantages we can develop the platform for blockchain based E-voting systems. The proposed platform provides a framework that can be implemented to conduct voting activity digitally through blockchain without involving any malpractices. Our goal is to create an E-voting system that can be trusted by voters and to encourage them to vote.

References

[1] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International journal of web and grid services 14, no. 4 (2018): 352-375.

[2] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[3] Viriyasitavat, Wattana, and Danupol Hoonsopon. "Blockchain characteristics and consensus in modern business processes." Journal of Industrial Information Integration 13 (2019): 32-39.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[5] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550, doi: 10.23919/MIPRO.2018.8400278.

[6] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.

[7] J. V. Cadiz, N. A. M. Mariscal and A. M. Ceniza-Canillo, "An Empirical Analysis Of Using Blockchain Technology In E-Voting Systems," 2021 1st International Conference in Information and Computing Research (iCORE), 2021, pp. 78-83, doi: 10.1109/iCORE54267.2021.00033.

[8] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in IEEE Access, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[9] A. M. Al-madani, A. T. Gaikwad, V. Mahale and Z. A. T. Ahmed, "Decentralised E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020, pp. 176-180, doi: 10.1109/ICSIDEMPC49020.2020.9299581.

[10] C. Angsuchotmetee, P. Setthawong and S. Udomviriyalanon, "BlockVOTE : An Architecture of a Blockchain-based Electronic Voting System," 2019 23rd International Computer Science and Engineering Conference (ICSEC), 2019, pp. 110-116, doi: 10.1109/ICSEC47112.2019.8974826.

[11] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 70746-70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[12] Z. Khudoykulov, U. Tojiakbarova, S. Bozorov and D. Ourbonalieva, "Blockchain Based E-Voting System: Open Issues and Challenges," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-5, doi: 10.1109/ICISCT52966.2021.9670245.

[13] Jafar, Uzma, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. 2021. "Blockchain for Electronic Voting System—Review and Open Research Challenges" Sensors 21, no. 17: 5874. https://doi.org/10.3390/s21175874.