

Block Chain-based E-Voting System using Smart Contract

Dr. Priya Shelke¹, Suruchi Dedgaonkar², Nilesh Gopale³, Rohit Desai⁴, Ninad Deogaonkar⁵ and Nachiket Joshi⁶

¹⁻⁶ Dept. of Information Technology, Vishwakarma Institute of Information Technology, Pune, India
Email: {priya.shelke, suruchi.dedgaonkar, nilesh.21910766, rohit.21910786, ninad.21910774, nachiket.21910799}@viit.ac.in

Abstract—Block chain is presenting new chances to develop new categories of digital services. Even though research on the topic is still in its early stages, it has mostly focused on the technical and legal challenges rather than utilizing this ground-breaking concept and creating better digital services. The study offers a novel block-chain based E-voting system that tackles some of the drawbacks of current systems and assesses some of the well-known block chain frameworks in order to build a block-chain based E-voting system. It has long been challenging to develop a secure electronic voting system that maintains the fairness and privacy of paper ballots while ensuring the transparency and flexibility afforded by electronic systems in current electoral schemes. We concretely assess the technology's potential by explaining a case study, including the election process and the implementation of a blockchain-based application that improves security and reduces the cost of holding national elections. A block chain is a type of distributed database that is this allows for the sharing of all data among all network users. By definition, a block chain system has several benefits that are suitable for electronic voting system. It is independent of a centralized server because its distributed architecture guarantees great system performance. Availability. Since each participant has full data, using the protocol, they may verify each block uploaded to the chain regarding the electronic voting system we propose, the double envelope encryption is combined here. Block chain technology and technique. This is the mechanism for turning the people's opinions into action in order to better manage system. Traditional elections have not pleased either the people or the government in recent years. They are not completely secure because ballots are easily tampered with. Additionally, it raises concerns about transparency and voter safety. Furthermore, it takes far too long to count the votes.

Index Terms— Voting, Block chain, Hashing of Fingerprint, Smart-Contract, Mining, Markle tree.

I. INTRODUCTION

Democratic voting is an important and rigorous mechanism in all regions. Countries typically vote using traditional the paper-ballots, mechanical devices, and electronic voting systems. [1] However, it requires new digital technology. Digital voting uses electronic voting machines, and there are two types of digital voting: electronic voting and I-voting. Electronic voting is when voters use their devices to vote at a vote center. I-voting needs a software interface because of this. The essential requirements for determining if a democratic process is legitimate include Accuracy, resilience against illegal conduct, efficiency, stability, and transparency of the

voting process. Digital voting methods can increase accuracy, confidentiality, and integrity while requiring less financial and human resources. Simply put, it makes sure that the votes cast and the outcomes are accurate [2]. Digital voting has certain disadvantages as well. False voting, cost-cutting, hastening results, and other unethical voting procedures are some examples. In fact, a number of unauthorized users could impair smart or IoT (Internet of Things) systems by materially altering voting or voting calculations in order to gain an advantage. A decentralized ledger that preserves a consistent perception of reality is block chain technology. Block chain is a peer-to-peer networking platform and mutual, tamper-proof ledger that has been utilized in cryptocurrencies like Bitcoin and Ethereum. In this instance, user anonymity is safeguarded by the public or private key's identification. There are numerous models built on the block chain that provide security and anonymity. Although block chain technology offers security, privacy, accountability, and durability, speed and scalability are the main implementation problems. Our team is developing a digital voting architecture that includes a smart contract to address the challenges of block voting adoption and ensure authentication, transparency, anonymity, accuracy, and autonomy, as well as uniqueness, integrity, and mobility. Based on the voter's information, a hash will be created in our system and placed in the chain [8]. Voters can remain anonymous because the data is hashed and kept in the block chain, which allows for scalability. Any modifications to the hash information will be quickly noticed. Smart contracts on the chain guarantee privacy and security. Smart contracts select miners to speed up transactions. Candidates are determined by many factors, including data transfer and power consumption. Each block has completed its voting procedure. The final vote count from the previous block can be simply evaluated. It reduces the amount of time spent counting.

II. RELATED WORK

A. Blockchain

Blockchain is a decentralized data management system in which data are spread across a peer-to-peer (P2P) network and subsequently stored in an encoded chain of blocks [3]. The electronic Bitcoin system put out by Satoshi Nakamoto is where the concept of blockchain was born [4].

These are some of the main characteristics of blockchain:

1. Keep the consensus mechanism in place, i.e., demand proof of work (POW) down the entire chain.
2. Put information into the blocks as a ledger.
3. Network-wide synchronization of the entire ledger.
4. Provides data Decentralization [5].

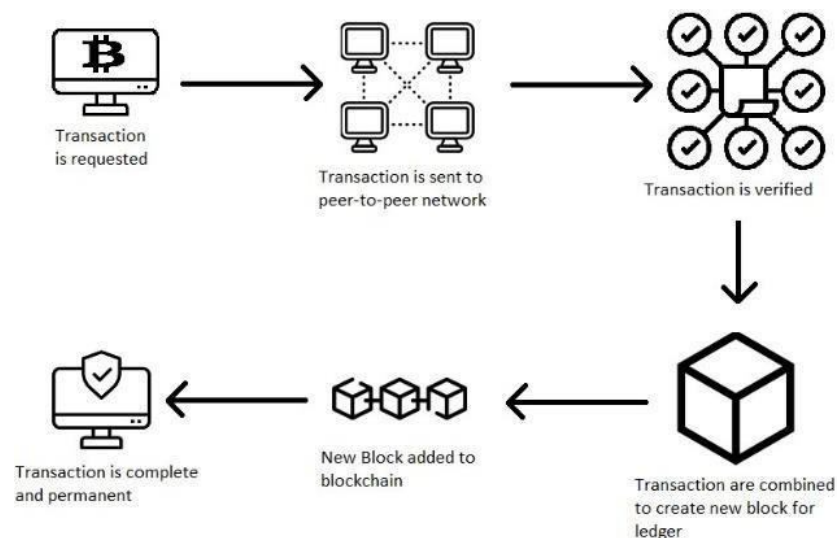


Figure 1. Flow of Transaction in Blockchain

Modern cryptocurrencies were developed in 2008 using the blockchain concept in conjunction with a number of other technologies and computing ideas. These digital currencies are rather than a centralized system or source, cryptosystems are used to secure data. Bitcoin was the first such blockchain-based cryptocurrency [6]. A cryptographic address is associated with information that represents electronic cash on the Bitcoin blockchain. Users of Bitcoins can digitally agree to and move ownership of that data to a different user, with a public record

of this transfer on the Bitcoin, enabling every connection user to independently confirm the authenticity of the exchanges. A dispersed group of individuals stores, upkeeps, and cooperatively manages the Bitcoin blockchain. Bitcoin deployments are typically developed with a specific objective or purpose in mind. Examples of these features include distributed ledger systems between businesses, cryptocurrencies, smart contracts (software loaded on a blockchain and executed by machines running that chain), and smart contracts themselves. A continual stream of innovations in the ledger technology sector have been made, and as the market landscape changes, new platforms are frequently unveiled.

B. Voting methods

In a democracy, there are several ways to cast a ballot. Many nations have switched from straightforward elections with ballots on paper to computerized voting machines over time. The following are the most popular techniques [7]:

1. Ballot Paper
 2. Vote over Internet
 3. Electronic voting Machine
 4. Biometric voting Machine
- **Ballot Paper:** The act of writing down your preferences on a piece of paper and submitting it is one of the most basic election mechanisms. This is referred to as ballot paper voting. In the table's first column, which is left vacant for voters to express their preferences, are the names of the candidates and the parties running in the election. The guidelines are quite basic. You can mark your choice of candidate with a cross, place the paper in the voting booth after folding it. The Ballot Box must be taken care of and monitored by the Election Authority in charge of overseeing the election [7].
 - **Vote over Internet:** With such a method, we can vote in the convenience of our own homes. Contrary to other internet-based services, this platform has received harsh criticism for the way it operates. The administration has repeatedly asked teams of cybersecurity specialists from around the world to evaluate its voting platform. The testing team has frequently come to the conclusion that not only can they alter the vote total, but they can also erase all evidence that they ever existed. There won't be any digital fingerprint that can be used to identify them in the system. [8] This has sparked considerable division among the populace. Justice for everyone was a key democratic principle. One of the major democratic celebrations is the right to vote. Therefore, it is the responsibility of the government to make sure that the public has complete faith in the system and that any problems are resolved.
 - **Electronic voting Machine:** The Ballot button on the control unit is pressed by the electoral authority in charge of overseeing the election, which initializes the EVMs. When a voter presses a button that corresponds to the candidate he wishes to support, the voting system will then turn on an LED light to let him know that the vote was accurately recorded. The machine then locks by itself. Now, when a new voter casts their ballot, the lock can only be opened by a fresh ballot number, which the person in charge will push once more. This will prevent a single person from casting numerous votes.
 - **Biometric voting Machine:** They devised a voting system based on fingerprints, where a biometric machine helps identify the voter. Numerous investigations have established the uniqueness of each person's fingerprint. When casting a vote, this can be used to identify the voter. The entire process concludes fast and painlessly. The government must establish a nationwide scheme for voter registration, whereby everyone is fingerprinted and a final list of all eligible voters is compiled. In conclusion, because voters can cast ballots from any location in the world, we may run into a similar authentication issue while designing a blockchain-based system. Thus, to ensure that the voters who cast their votes are authentic, we may utilize biometric sensors or even face recognition software. [7]

C. EVM

Voting is done using electronic machines, and a voting method is introduced. This system is centralized. Voting data can be easily changed in this way. There is no system in place for voters to check the accuracy of their vote. [9] Describe a voting system based on block chain in which each EVM is directly connected to another EVM in a network. This method has three parts: peer verification transactions, chain manipulation detection, and fingerprint authentication. It is subject to DoS (Denial- of-Service) attacks and eavesdropping.

D. Blockchain Based E-voting

Due to the rise in popularity of currencies, blockchain, the technology that underpins them, is receiving increased attention from researchers. Numerous e-voting methods have been implemented in conjunction with blockchain.

Electronic voting is the term used to describe voting that relies on gear or software that is electronic. Such systems may be able to support/implement a wide range of tasks, from the voting process' startup to the storage of votes. There are many different types of method, including computers, mobile devices, and kiosks seen at voting offices [10].

For government and organizations to polling devices, Agora was created. It is an end-to-end verifiable blockchain-based voting system. Agora used tokens to identify eligible voters in elections, and each eligible voter received a token from an institution. However, in order to oversee the voting process, each of these methods leaned on reliable outside sources. The third party could collaborate with the candidates to manipulate the election. Additionally, the public can access and see the data that is kept in the blockchain. This compromises the security and dependability of Using block chain for voting.

Blockchain-based voting's protocols incorporate smart contracts and encryption algorithms to address this issue. The third party was typically replaced using smart contracts. Smart contracts enabled the Open Vote Network, an identity protocol. The following procedures were part of the E- voting systems: The first stage is voter registration (registration). Officials check voters' IDs on election day (verification and authentication). People who are qualified to vote may do so in the following phase (casting collation). The vote ought to be verified and encrypted. The votes' correctness, confidentiality, and anonymity must all be ensured and cannot be modified in any manner. The final step in the counting process for electronic voting systems is to add up all the votes in accordance with the design (counting display of results). The majority of e- voting applications use central authority control. Such systems have a number of shortcomings and perceived hazards. The majority of e-voting applications use centralized government control. Such systems have a number of shortcomings and perceived hazards. For instance, there are no standards for electronic voting systems, security and reliability risks, fraud and hacker vulnerabilities, expensive machine costs, and insecure transaction storage.

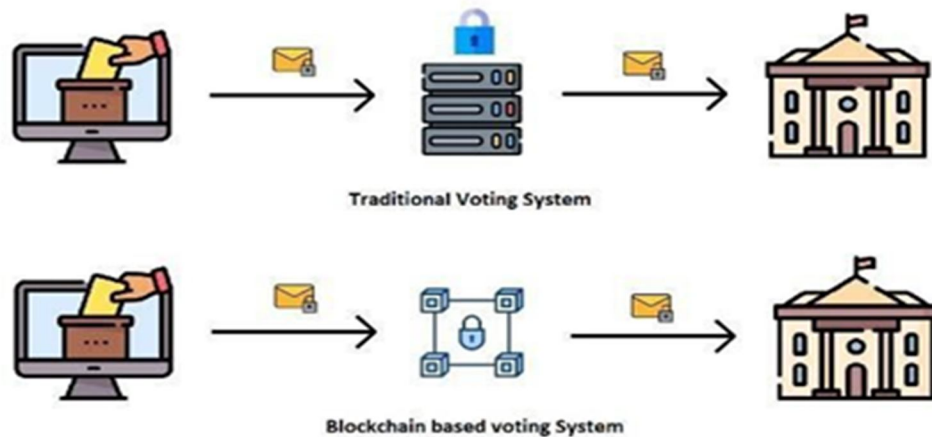


Figure 2. Block-chain based E-Voting System

E. E-voting Systems process

- Setup: Enter the security parameters or values, then encrypt (or decode) the processes after producing the private (or public) pair of keys.
- Register: Give the identifiers as IDs to generate the secret (or public) passcode as an output [11].
- Vote: After establishing a vote element or component, the electors calculate the cypher text and matching approval.
 - o Credible: This helps to authenticate voting is integrity in the election server by selecting the input as a vote.
 - o Validate Vote: Following the voting phase, voters may submit requests for the bitcoin contracts they voted at the time of polling advertising is occurring, and by entering the public parameters, voter status, and privacy information, they could confirm the outcomes given. Results the other legitimate or untrue when they are returned.
 - o Counting up: After all votes have been cast and verified, the results are tallied with the input being the necessary secret key and the output being the polled box element. The system returns False if the result is incorrect.
 - o Verify: When the publicity phase's public parameters are entered, a vote is authenticated as having been cast in accordance with the ballot's outcome in a valid and accurate manner. [12]

III. PROPOSED VOTING MECHANISM

A. Data Management of the system

Huge amount of data is generated during the election process. As a result, data should be collected in a systematic manner. As shown, our system employs two types of storage- Database Storage and Cloud Storage.

B. Voter Registration

- Each person must visit their local voter registration office and submit the required documentation in order to cast a valid ballot.
- A set of public and private keys will be created using a key creation method.
- In the block chain network, voters are identified using their public key. The voter's mobile phone numbers receive the secret key. They can use this private key to cast a ballot and take part in the voting system.
- The hash is generated from voter's submitted fingerprint and the algorithm used is fingerprint hash generation. The whole procedure of creating hashes from data provided by voters is shown. [2]
- To create a new hash value, the created hash will be coupled with the voter's other information.
- The final hash value will serve as a voter list in the block chain's genesis block.
, where hash value = membership proof.

C. Voting with a smart contract

The following are the functions of smart contracts running on the block chain:

- **Voter Verification:**
 - Using an internet-connected device, the voter logs into the voting system with their private key.
 - Submit your fingerprint, NID, and other data.
 - In the genesis block, smart contracts created on the block chain compare the information provided by the valid voter to the information submitted.
 - If the data matches, a list of candidates is shown to the voter. [13]
- **Make a Casted vote block:**
 - The voter selects one of the candidates from the list and votes.
 - Use a digital signature to sign the vote, then send the transaction to the smart contract (SC).
 - For each vote cast by the voter, smart contract creates a Voter ID for Identification of each vote.
- Increase the number of votes cast for the chosen candidate. Make a block containing the transactions made by the voter, together with their VID and Candidate Vote number. [2]
- **Selection of Miner:**
 - A miner selection algorithm is run by the SC.
 - In order to prevent record interference, all miners compete to generate outcome of the block's hash first in Bitcoin, which requires a significant amount of processing power. It has been suggested that the voting architecture choose a Miner based on heuristics extrapolated from that Miner's accomplishments. The SC compiles factors such node capacity, energy use, and delay. [5]

IV. CONCLUSION

Securing vote security is a challenge for many nations. To guarantee voter participation and validity, the security of vote data, and the accurate measurement of votes, a smart contract-based block chain- based voting system can be developed. In order to cut down on computational expenses, this technique entails the SC providing voter authentication and participating in the choice of a Miner in the Block chain. Additionally, it promptly counts the votes, speeding up the election process. Citizens can vote using smart devices from anywhere thanks to this mechanism. This will help to raise the number of voters needed to establish democracy in any nation. The objective of this project is to develop an encryption method that will increase the security of our system in the future.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their useful suggestions that helped in improving the quality of this paper. We would also like to thank Vishwakarma Institute of Information Technology, Pune for supporting this work.

REFERENCES

- [1] F. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-based e-voting system," in 2018 IEEE 11th international conference on cloud computing (CLOUD), 2018.
- [2] B. L. J. K. S. A. N. S. S. R. R. P. Yu and M. H. Au, "Platform-independent secure blockchain-based voting system," in Information Security: 21st International Conference, Guildford, UK, 2018.
- [3] K. M. Khan, J. Arshad and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, pp. 13--26, 2020.
- [4] A. Alam, S. Z. U. Rashid, M. A. Salam and A. Islam, "Towards blockchain-based e-voting system," 2018 international conference on innovations in science, engineering and technology (ICISSET), pp. 351--354, 2018.
- [5] Fatrah, S. El Kafhali, A. Haqiq and K. Salah, "Proof of concept blockchain-based voting system," in Proceedings of the 4th International Conference on Big Data and Internet of Things, 2019.
- [6] P. Baudier, G. Kondrateva, C. Ammi and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technological Forecasting and Social Change*, vol. 162, p. 120397, 2021.
- [7] Y. Soni, L. Maglaras and M. A. Ferrag, "Blockchain based voting systems," in European Conference on Cyber Warfare and Security, 2020.
- [8] M. a. P.-M. A. Pawlak and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Computer Science*, vol. 141, pp. 239--246, 2018.
- [9] Li, J. Xiao, X. Dai and H. Jin, "AMVchain: authority management mechanism on blockchain-based voting systems," *Peer-to-peer Networking and Applications*, vol. 14, pp. 2801--2812, 2021.
- [10] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020.
- [11] J.-H. Hsiao, R. Tso, C.-M. Chen and M.-E. Wu, "Decentralized E-Voting Systems Based on the Blockchain Technology," in *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17*, 2018.
- [12] Y. Abuidris, R. Kumar, T. Yang and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *Etri Journal*, vol. 43, no. 2, pp. 357--370, 2021.
- [13] 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.