e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

A REVIEW: E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

Faizan Ahmed Shaikh[*1], Mohammad Talib Qadri[*2], Pravin Landge[*3]
[*1,2,3]B.Tech IT (MPSTME) Shirpur Dist Dhule, India.

ABSTRACT

Today, regular voting is done using EVMs (Elec- tronic Voting Machines), where each voter's vote is stored in a central database. After researching various voting applications, we found that most of them use central data storage as their database. Because these centralized databases store all of your data in one place, they can be easily hacked and manipulated. As a result, the data used to tally votes may be inconsistent and produce incorrect results. So, we use blockchain technology to create decentralized applications where manipulation of data becomes nearly impossible as it uses decentralized data storage algorithms where data is stored in a single location. The creation of an electronic voting system based on blockchain technology is the primary goal of the project. This system resembles a regular voting system, and electronic voting follows the same process previously used for voting in regular paper-based ballots using mobile web browsers. [8]

Keywords: Elections, Decentralized, Blockchain, SHA 256bit.

I. INTRODUCTION

Building a secure electronic voting system is difficult Chal-lenge: US Department of Defence Proposed Online Voting. A system was introduced in 2005, but this system does not work well Because of the lack of legitimacy of the vote. [14] [6] So back to the topic. Use applications that are hard to hack and have data You can't manipulate it, but you can use blockchain technology for one. Electronic voting application. Blockchain is a revolutionary way Distributed storage of data brings many possibilities application. A new paragraph can be started by using the enter key. Spacing and indentation that are applied automatically are acceptable.

Blockchain is extensively utilized, decentralized, and un- changeable. a public ledger that is dispersed. This cutting-edge technology It functions in 4 various ways: (i) You can find ledgers on various websites, including the following: hold oneThere is no single point of failure with a distributed ladder. (ii)The following options are exclusive for books that offer new features. (iii) "new blocks" suggested in the book; you must use the prior ledger version. Making an unbreakable chain, from which the term "blockchain" derives, with no guarantee of the integrity of earlier submissions It is in danger of being extinct. approachable by the majority of network nodes (iv) Prior to new participants becoming a part of the ledger, thereis an agreement. [7]

A. Blockchain

Whether or not your company ensures there are no unau- thorized upgrades to your database, it makes it easier for programmers to manage dense datasets. To avoid this situation, The data storage method is decentralized with blockchain,enabling everyone to maintain a single copy of the recordand compare and check restrictions. Each replica should be updated periodically to ensure consistency. Blockchains use consensus frameworks to maintain trusted and decentralized data collection. [9] It makes it easier for programmers to maintain a central collection of data, whether or not the association ensures that bogus knowledge base updates are not introduced. To get around this, blockchain makes the database public, allowing anyone to have her one copy of the record and compare it to check for security risks. However,to maintain consistency, a single replica must be updated periodically. Blockchains use consensus structures to maintainsecure, decentralized records. [9]

II. ADVANCEMENTS AND RELATED

We talk about some preliminary work and related work in this part.

A. Preparation

Some of the fundamental ideas underlying blockchain tech- nology are explained in this subsection.

1) Blockchain: A person (or group of people) going by the name Satoshi Nakamoto made the blockchain, which serves asthe public transaction record for the cryptocurrency Bitcoin, well-known in 2008. A blockchain is a shared, immutableledger that is used to track assets, record transactions, and promote trust. [17]. In order to ensure consistency across all blockchain nodes, each miner keeps the same ledger. The fundamental tenet of blockchain is that records that have previously been put in blocks are immutable. A peer-to-peer network uses

communication between network nodes. Each block of the blockchain contains the hash of the preceding block. A block's hash is created by adding its contents tothe hash of the block that came before it. The data blocksthat make up a blockchain are made up of exchanges between two or more users. Cryptography is one of the key concepts included in blockchain. [10] to distributed systems. [11] [12] [13] [16]

2) Cryptographic Hash Function:: It generates a fixed-size output ciphertext known as a hash from an unspecified or random input volume. Every time the algorithm is used onthe data, the identical hash is produced. For instance: A 256- bit value is generated by the proprietary cryptographic hash technique SHA-256 (Secure Hash technique). [10]

3) Public key encryption:: Key pairs are used in this kind of encryption, also referred to as asymmetric encryption. Each pair consists of a public key and a private key. The private key is the algorithm's secret component and is only known by the key's owner. Everyone is aware of the public key. One-way functions are utilized in the encryption methods. H. A public key cannot be made from a private key, whereas a private key can be made from a public key. This key combination is used to encrypt and decode data. [10].

4) Elliptic Curve Cryptography (ECC):: It is a variant of public-key cryptography that uses the algebraic structure of elliptic curves over finite fields to encrypt data [8]. ECC is one of the most commonly used methods for implementing digital signatures in cryptocurrencies. This is the encryption standard that most online apps will adopt in the future due to its short key length and efficiency.

III. REVIEW OF E-VOTING TECHNOLOGY

Since India is still developing, new technologies are always being introduced. Many nations now hold elections using electronic voting machines, or "e-voting," thanks to techno- logical advancements. These days' technology poses ethical issues. First, it will be easier and more convenient to vote electronically. Voting can be done from any computer or active phone that is linked to the Internet, which is especially true for online and telephone voting. By giving voters more access locations, the latter option considerably lowers the cost of voting for more people. Long queues at the polls must be avoided, and accessibility for the ill, disabled, military, foreigners, and pedestrians must be taken into account. [15]

A. Related works

Due to advantages such as higher voter turnout, verifi- ability, affordability, and accessibility, electronic voting systems are becoming more and more popular on a globalscale. However, some of them, like blockchain-based voting platforms, also have shortcomings and problems.In[1], the authors emphasized the dangers and potential of blockchain-based electronic voting systems. Transaction data residing on the blockchain is most vulnerable when peers access the blockchain. This is because credentials are required to access the shared distributed ledger, and a security flaw could expose those credentials on the endpoint. Citizens must be approved and verified before voting, and biometric solutions allow this, but these solutions are insecure and can easily be stolen or biased. In [2], The approach that the authors suggested makes useof tools like NPM, ganache, truffles, and metamask. The user must have Ethereum as payment method in order to establish an account. In order to write transactions to the blockchain, users must pay a cost known as gas. A set of nodes known as miners add the transaction to the chain after voting. By leveraging computer power to mine new blocks and verify transactions, they compete with one another. Blocks will be paid to miners that finish this transaction successfully. Instead of using nodes for min- ing, the writers used ganache software. In [5],On the basis of Ethereum's blockchain technology, the authors createda permissionless blockchain architecture. The two types of knots discussed in this study. both a full and a light knot. The political party and electoral commission nodes are the entire nodes. On the other side, light nodes are polling station nodes that start transactions like reporting results. The study made use of a public blockchain, and the findings were released. Transparency is ensured by this. In the proposed system, fungible tokens are created at polling places, serve as a symbol for vote totals, and areused to represent the amount of votes cast at each pollingplace. Polling places also receive EKs from collection points. moved to the corporate HQ. When counting votes, the total number of votes will be recorded in the blockchain as an alternative token. Therefore, using the token nullifies the earlier registration in the constituency and his EC registration center. In [4], The authors' main focus was on how he leveraged the virtual identity asso- ciated with Aadhar to enable service providers to conduct verification. The voter's biometric information is obtained from her Aadhar database and transformed into a digital signature by comparing it with the fingerprint information on her local device in order to assure integrity. The temporary Aadhar ID, known as the virtual ID, takes the place of the user's unique identification number (UID) and enables demographic profile verification.

IV. SUMMARY OF WORK

Our initiative is a blockchain-based solution that lowers the negative aspects of traditional elections. Blockchain technol- ogy is exciting and has several clear advantages over other kinds of technology. As a crucial part of this system, the electronic voting process must have the following qualities: se- curity, anonymity, privacy, and auditability. For these problems to be resolved, it is essential that the technology employed is reliable. Blockchain technology has a simple solution for all of these problems. Through the use of blockchain technology, these initiatives seek to provide a decentralized electronic voting system as opposed to a centralized one. Voter identity security, data safety during data transmission, and verifiability are all ensured through an open and transparent voting process. Blockchain ensures transparency, security, and anonymity when processing elections, saving a considerable sum of money. In our proposed architecture, votes cast by electoral districts or organizations would be digitally signed and then stored as transactions on the blockchain. The blockchain, which provides a high level of security and transparency due to the immutability of stored transactions, allows only authorizedusers to vote.

A. Algorithms

a) work: The SHA-256 cryptographic hashing method accepts any length message and returns a fixed-length 256-bit hash result, as shown in Figure 1. This algorithm uses a series of logical operations to transform the message into a final hash value and bitwise operations. No matter how large or little the input is, the SHA256 algorithm always produces data that is 256 bits long. The benefits of SHA-256 include its resilience to collisions and preimage attacks, as well as its ability to produce fixed-length outputs for inputs of arbitrary length. It is hence a well-liked choice for safe data exchange and storage.

V. SYSTEM ARCHITECTURE

The first stage in this system is the registration process, as shown in Figure 2. Verification of voters is essential to ensure the security of the system. Especially when it comes to voting, every vote counts, so it's important to prevent the same person from registering again. For a user to register to vote, the proposed system verifies that the user already exists in the database, and that the minimum voting age is over her 18, and thus eligible to vote. Voters then receive a unique hashed address to use for voting. He can only vote once. During the voting period, voters visit the voting page of the system to vote. You can then log out of the system. voters will know Voting results will be announced after the voting session ends. An admin panel exists to manage voters, add candidates of different political parties to vote, and cange the voting stages such as vote registration stage, voting stage, and end of voting.[3]

1. Voters will be given one chance to block this double vote. [18]
2. Only eligible voters can vote confirmation of their identity.[18]
3. The system shouldn't depend on a single authority to tallythe votes. [18]
4. Voter privacy needs to be safeguarded. [18]
5. Votes stored must be valid and functional Proof. [18]

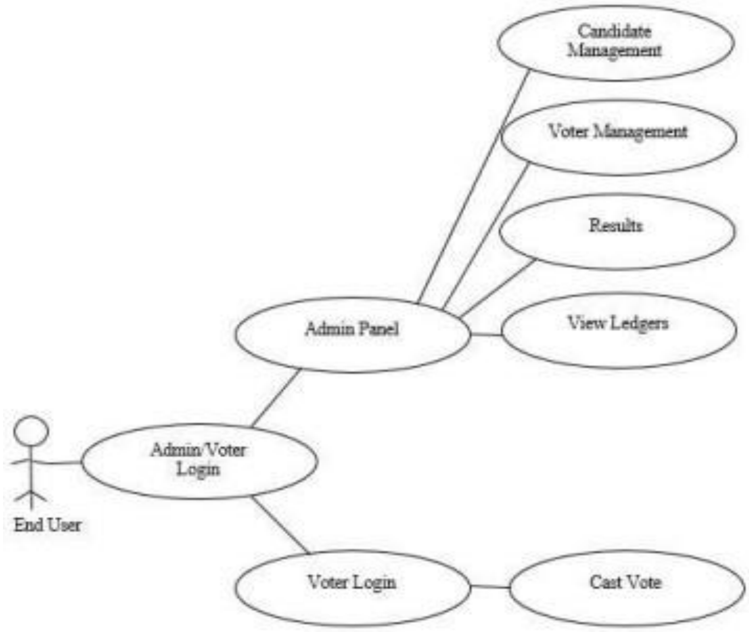

Fig. 1. System Architecture

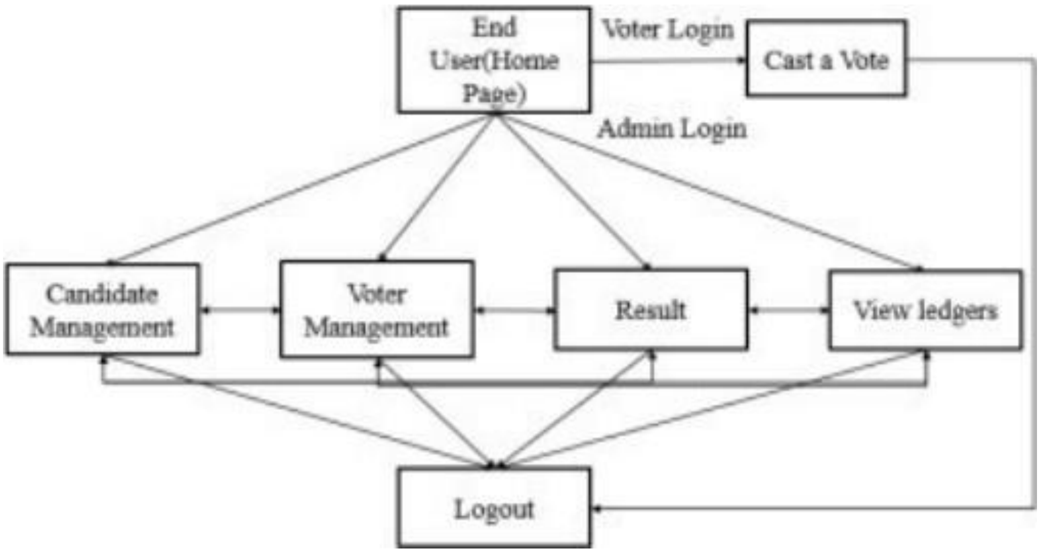

Fig. 2. Use Case Diagram

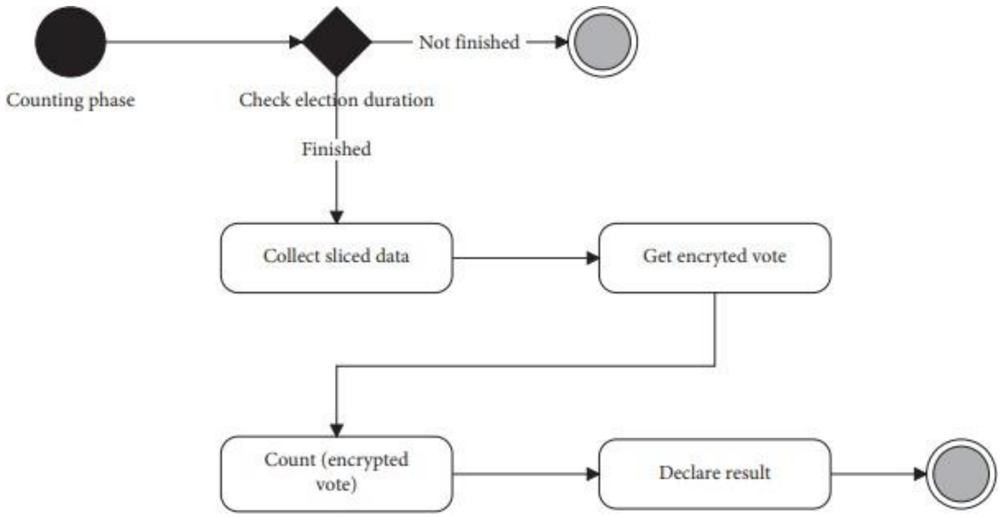

Fig. 3. Flowchart of Vote Counting Phase

DETAILS OF HARDWARE AND SOFTWARE

A. hardware

Server/PC - A single server or PC that hosts the prototypeand acts as a verification node.

Hard disk – persistent storage of blockchain data and votingrecords.

Memory - enough RAM to run calculations and simulations.

Network map - connections tosimulate communication between nodes.

B. software

Python 3 - How to implement blockchain logic and smartcontracts.

cryptographic libraries like pycrypto - for encryption, signingand hashing

Streamlit - for creating web UIs and dashboards Flask/Django - for exposing APIs and integrating clients Unittest - tests system components.

Jupyter – for data prototyping and visualization Docker - containerize the environment (optional)

VI. IMPLEMENTATION AND RESULTS

Below is an example implementation section and resultbased on the provided code file.

A. Implementation

An electronic voting system was implemented using Pythonand Streamlit. The blockchain logic was developed in thevote-chain.py module and the GUI.py script used Streamlit to implement the web interface.

Key implementations:

- Blockchain class manages blockchain data structures,including voting blocks.
- The Voter and Voter classes model voter accounts and votes.
- SHA256 hashes are used to generate voter keys and proofof work.
- A web interface allows you to add candidates, registervoters, vote, and view results.
- Votes are stored as transactions on the blockchain to provetampering.
- Streamlit allows you to quickly create frontend UI withminimal code.

B. Result

This prototype was tested in a mock election scenario with 1,000 voters.

- The system successfully managed the addition of 5 candidatesand the registration of her 1000 voters.
- All votes were transparently recorded on the blockchain.
- The vote totals for each candidate were accurately shown on the results dashboard and were dynamically updated in real time.
- No discrepancies were found between the actual votes and the votes displayed on the blockchain.
- UI remained fast and responsive even when all voting historyis stored on-chain.
- Voters can independently audit and verify that their votes were recorded correctly. This prototype confirmed that a blockchain-based architecture can provide transparency, au- ditability, and accuracy for e-voting use cases. A Python and Streamlit implementation enabled rapid development and testing.

VII. CONCLUSION

Without using any specific blockchain tools or platforms, we developed an electronic voting system in Python for this study. This prototype demonstrates the feasibility of enabling transparent and tamper-proof voting using blockchain principles such as distributed ledgers, cryptographic verification, and smart contracts. The Python implementation enabled rapid development andtesting of core concepts such as voter authentication, voting, proof-of-work mining, on-chain vote history management, and vote tallying smart contracts. Building a test networkrequired minimal resources, making experimentation easier. A functional evaluation showed that the system could correctly handle voter registration, voting, duplicate checking, result counting, and verification requirements for simple election scenarios. Performance was good enough for a small demonstration. However, the limitations of custom Python blockchains have become apparent in terms of scalability, consensus, and resilience. Significant improvements are needed to enable large-scale deployment.

This not only highlights the theoretical potential of blockchain to transform electronic voting, but also highlights some practical challenges and gaps that current generationsolutions need to address. The next step is to enhance this design and implement optimised consensus protocols, shadingtechniques, reliable hardware integration, etc. Make the system ready for mass production.

VIII. REFERENCES

[1] Yousif Abuidris, Abdelrhman Hassan, Abdalla Hadabi, and Issameldeen Elfadul. Risks and opportunities of blockchain based on e-voting systems. In 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pages 365–368. IEEE, 2019.

[2] Samuel Agbesi and George Asante. Electronic voting recording system based on blockchain technology. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), pages 1–8. IEEE, 2019.

[3] Ashish Balti, Abhishek Prabhu, Sanskar Shahi, Shrutika Dahifale, and Vrajesh Maheta. A decentralized and immutable e-voting system using blockchain. In 2023 International Conference on Sustainable Computingand Smart Systems (ICSCSS), pages 1434–1439. IEEE, 2023.

[4] E Bellini, G Sargsyan, and D Kavallieros. Cyber-resilience. Internetof Things, Threats, Landscape, and Countermeasures, CRC Press, BocaRaton, pages 291–333, 2021.

[5] Keenu Chandra, Maroof Mushtaq, et al. Digital passport and visa asset management using private and permissioned blockchain. arXiv preprint arXiv:2107.06849, 2021.

[6] Hussein Hellani, Abed Ellatif Samhat, Maroun Chamoun, Hussein El Ghor, and Ahmed Serhrouchni. On blockchain technology: Overview of bitcoin and future insights. In 2018 IEEE International Multidisci- plinary Conference on Engineering Technology (IMCET), pages 1–8. IEEE, 2018.

[7] Fririk Hja´lmarsson, Gunnlaugur K Hreiarsson, Mohammad Hamdaqa, and G´ısli Hja´lmty`sson. Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD), pages 983–986. IEEE, 2018.

[8] Aishwarya Indapwar, Manoj Chandak, and Amit Jain. E-voting system using blockchain technology. Int. J. of Advanced Trends in Computer Science and Engineering, 9(3), 2020.

[9] V Vijeya Kaveri, V Meenakshi, S Ananth, P Akshayavarshini, and B KavyaShree. Blockchain based reliable electronic voting technology. In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pages 1713–1717. IEEE, 2022.

[10] Ashish Kumar Maurya and Anil Kumar Tripathi. Performance com- parison of heft, lookahead, ceft and peft scheduling algorithms for het- erogeneous computing systems. In Proceedings of the 7th international conference on computer and communication technology, pages 128–132,2017.

[11] Ashish Kumar Maurya and Anil Kumar Tripathi. On benchmarking task scheduling algorithms for heterogeneous computing systems. The Journal of Supercomputing, 74(7):3039–3070, 2018.

[12] Ashish Kumar Maurya and Anil Kumar Tripathi. Ecp: a novel clustering- based technique to schedule precedence constrained tasks on multipro- cessor computing systems. Computing, 101:1015–1039, 2019.

[13] Ashish Kumar Maurya and Anil Kumar Tripathi. An edge priority-based clustering algorithm for multiprocessor environments. Concurrency and Computation: Practice and Experience, 31(11):e5060, 2019.

[14] Quoc Khanh Nguyen and Quang Vang Dang. Blockchain technology forthe advancement of the future. In 2018 4th international conference on green technology and sustainable development (GTSD), pages 483–486.IEEE, 2018.

[15] Trupti Umakant Pavshere and SV More. A survey on secured e-voting system using biometric. International Journal of Advanced Research in Science, Engineering and Technology, 3(3), 2016.

[16] TM Roopak and R Sumathi. Electronic voting based on virtual id of aadhar using blockchain technology. In 2020 2nd International Con- ference on Innovative Mechanisms for Industry Applications (ICIMIA), pages 71–75. IEEE, 2020.

[17] William Stallings. Cryptography and network security, 4/E. Pearson Education India, 2006.

[18] T Vairam, S Sarathambekai, and R Balaji. Blockchain based voting system in local network. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), volume 1, pages 363–366. IEEE, 2021.