Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2023)
IEEE Xplore Part Number: CFP23CV1-ART; ISBN: 978-1-6654-7451-1

2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) | 978-1-6654-7451-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/IDCIoT56793.2023.10053410

Designing a Blockchain-Enabled Methodology for Secure Online Voting System

Saurabh Singh
Department of ITCA
Madan Mohan Malaviya University of Technology
Gorakhpur, India
saurabhthakur321jnp@gmail.com

Alisha Singh
Department of ITCA
Madan Mohan Malaviya University of Technology
Gorakhpur, India
kavya091100@gmail.com

Shivam Verma
Department of ITCA
Madan Mohan Malaviya University of Technology
Gorakhpur, India
shivam7052128830@gmail.com

Rajendra Kumar Dwivedi
Department of ITCA
Madan Mohan Malaviya University of Technology
Gorakhpur, India
rajendra.gkp@gmail.com

***Abstract*—Blockchain has built-in security features. Basic concepts in blockchain include cryptographic, decentralized, and consensus concepts that guarantee integrity. It's been extremely difficult for a very long time to create a safe and secure electronic voting system that gives the clarity and versatility provided by electronic systems, as well as the transparency and privacy supplied by present voting systems. In this research work, blockchain application is assessed for implementing decentralized electronic voting systems. The study offers a different electronic voting system based on blockchain that tackles some of the drawbacks and limitations of current systems and assesses some of the well-known blockchain frameworks in order to build a blockchain-based e-voting system. Through the analysis of a case study, the possibilities of distributed ledger technology have been specifically evaluated.**

Keywords— Blockchain, Electronic Voting (e-voting), Electronic Voting Machine (EVM), Smart Contract, Secured-voting, Decentralized ledger

I. INTRODUCTION

Democracy aims to protect citizens from discrimination by sharing equal rights irrespective of caste, creed, religion, or gender. In a democracy, people choose their leader independently in elections through the voting System provided by the Election commission of that particular country. But what if these systems are flawed and people don't trust them, then what is the use and point of democracy? Not only this but nowadays various measures are being taken for cost-effective and secure voting systems. Here blockchain comes into the picture, so it is basically a technology that deals with the fault in the electronic voting system which is currently being faced by citizens.

A. Motivation

With the concept of blockchain, this study proposed a novel system, which will ensure that no third-party interrupts (even not the Election commission itself) and the vital part is that it will be end-to-end verifiable [1]. The name "blockchain" itself suggests that it is a chain of blocks, which means that various new blocks are created and each block contains a hash (a unique key) [2], [7]. The advantage is that whenever the data will be altered or modified in any one block, the hash key corresponding to that particular data will also change similarly there are millions of blocks, and the hash would be changed in each one of them which will change the whole data [3]. In this way, any kind of suspicious activity can be detected.

Without question, the constantly evolving blockchain technology that serves as the foundation for the well-known cryptocurrency Bitcoin hastened the dawn of a new age for the Internet and online services [20]. While the majority of people only pay attention to bitcoin and other cryptocurrencies, there are actually many administrative and fintech operations that could previously only be performed online or offline that can now be safely moved to the Internet as online services thanks to the immutability of the blockchain. Because of smart contracts and other features that surpass traditional systems, a blockchain is a powerful tool.[4], [5].

In this research, the issues with the voting methods were examined, and an online voting model was proposed in an effort to address these issues. For a high-end-to-end system that provides privacy and security, hashing algorithm approach, block generation and sealing, information gathering, and outcome declaration through a versatile blockchain technique are needed. In this research paper, a digital voting system is proposed that utilizes the Ethereum Blockchain to generate a wallet with the user's accreditation. Blockchain maintains voter confidentiality while yet being accessible to the general public [6], [8]. The suggested voting mechanism takes advantage of a more reliable, cost-efficient, and tamper-proof blockchain. This study would also broaden the restrictions placed on the structure, engineering, design, and application of the current voting system.

B. Contribution

Following are some contributions made by this paper:

- Concept of decentralization has been used such that there exist different networks and data for different systems.
- With the help of smart contracts, the involvement of third parties can be avoided.
- Distributed ledger technologies help in storing information in a secure manner using cryptography.

C. Organization

The rest of the paper is divided into the following sections: Section II has a description of Electronic Voting and Blockchain Preliminaries; Section III contains the literature review (followed by surveys and a summary table); Section IV ponders over the proposed system; Section V describes the implementation, evaluation, and results; At last, Section VI winds ups the whole paper.

II. E-VOTING AND BLOCKCHAIN PRELIMINARIES

In this part, we initially go into further detail on the design factors to take into account while building an e-voting system. And after that, we give a general review of blockchain and smart contract technologies and their suitability for building an electronic voting system.

A. Design Consideration

We formulated the below set of prerequisites for a workable electronic-voting system after evaluating both the criteria for these models to be used efficiently in a national election of a country and the current electronic voting systems. Coerced voting shouldn't be possible in an electoral system. A voting system ought to include a technique for safe authentication using an id (identity) verification service. whereas a voting machine shouldn't permit the linking of votes to specific voters. An election system must promote openness by giving each voter the verifiable certainty that their vote was tallied fairly and without jeopardizing their right to privacy. The voting mechanism ought to make it impossible for outsiders to meddle with any votes.

B. Blockchain as a service

In a distributed ledger that cannot be altered or destroyed, data is saved in the blockchain. The ledger is now impervious to change. The blocks are chained to ensure immutability, and every block holds a hash that depends on the preceding block and, by induction, the full prior chain [18]. There are two distinct blockchain types.

The ability to read or interact with a blockchain is finite to a private blockchain. Private blockchains are sometimes referred to as permissioned blockchains since only certain nodes are allowed to connect with them [19]. Including cryptocurrencies, blockchain offers an interface for creating decentralized and immutable apps and smart contracts.

Preprogrammed agreements known as smart contracts come into effect when certain criteria are met. Smart contracts, like regular written contracts, are used as necessary agreements between the parties [20]. By automating transactions and enabling direct, automatic agreement-making between parties, smart contracts do away with the necessity for an intermediary [21].

III. LITERATURE REVIEW

This section contains a detailed summary of previous studies on this particular subject. This also inspects academic books, papers, and other source materials that are relevant to a particular area of research. It also includes previous and significant works in the field of this research.

Anasune et al. [10] proposed an approach that will assist in developing a system that will address current and prospective difficulties and do away with the shortcomings of these earlier systems. By implementing blockchain in the dispersion of datasets on e-voting systems, one of the fraudulent causes of database manipulation can be reduced [17]. We're going to utilize the AES technique to encrypt the data we downloaded from the fingerprint sensor. This study examines the use of a blockchain algorithm to record election results across all locations. Rahardjo et al. [14]; this recording system takes place after the vote. This recording system is safer and more trustworthy thanks to the utilization of hash values and digital signatures while recording the outcomes of each voting station that is linked to the others. E. Sakhamuri et.al.[13] suggested security evaluation of the voting equipment in India. From an unnamed source, a Real Indian EVM Security Review was compiled. According to the report, EVMs are susceptible to strong attacks that could change the results and jeopardize the confidentiality of the vote. Using Modified Blockchain Technology for Trustworthy Electronic Voting was proposed by Crowcroft et al. [11].

TABLE 1. COMPARATIVE ANALYSIS OF EXISTING WORK

Author	Issues	Techniques used	Research gaps
Kelapure et al. [16]	Not that good for tough application .	Cryptographic verification	It is not compatible with sophisticated apps.
Khoury et al. [10]	This can't remove the need for external anchors.	Decentralisation	External trust anchors are still required despite the existence of blockchains.
Bhavan et al. [14]	Verification is not good.	AES Algorithm	Security protocol verification is subpar.
Rahardjo et al. [13]	Only provided a review of a voting system.	SHA-26 algorithm	They solely conduct reviews of the e-voting system rather than implementing surveys.
Cao-Minh et al. [11]	They give feedback on past and present e-voting systems.	Ethereum network	Offers an analysis of the past and present voting systems.
Hreiðarsson et al. [9]	Allows for revoting	quorum	Revoting is permitted under the Estonian system.
Gibson et al. [12]	Doesn't offer a quicker voting experience	Cryptography	They are unable to address design choices that facilitate faster voting.
Boucher et al. [15]	Doesn't tell specifically about the protocols for elections.	decentralization	They make no mention of election procedures in member states.

This study proposes a system that uses suitable hashing techniques to guarantee data security.

IV. PROPOSED SYSTEM

The current online voting system would be redesigned with Blockchain technology added. In comparison to the current system, which was detailed on the previous page, the suggested system provides the following advantages. Users' can vote from anywhere in the world until they possess citizenship of the country. The voting is stored in the Blockchain which makes it tamper-proof. As there's no standing in queue for casting vote it will save a lot of time and reduce the workload. We have worked on the following ideas by having two different sets of modules: the election commission and the voter(s).

Elections are created by the Election Commission, which also adds registered candidates and parties to fight them. The information is shown to the voter's front end for voting utilizing a REST API of election housed on Ethereum's Blockchain. The Election Commission then retrieves the vote count from our blockchain infrastructure once the vote has been cast. The drawback of not using the conventional approach to smart contracts is that the blockchain framework we developed cannot operate on the main net because it must be hosted and a different web 3.0 provider must be used to interact with it. Additionally, the lack of a public API for voter ID results in the inability to authenticate a voter.

A. Blockchain setup

Voters must cast their ballots in a controlled setting in order to meet the safety and privacy standards for electronic voting and to guarantee that compelled voting is not possible.

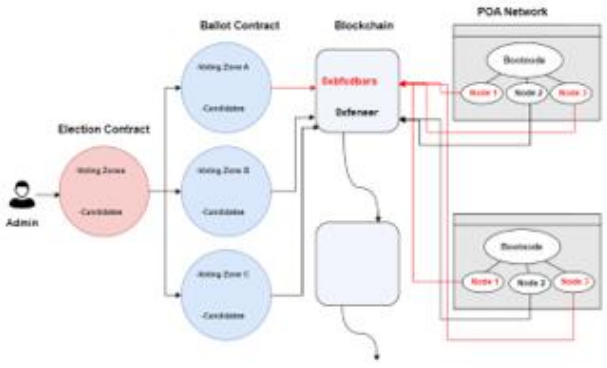

Fig 1: Election Process as a Smart Contract

There are two basic categories of nodes that make up the blockchain's structure.

(i). District Node:

Represents each electoral ward. There is a software agent on each district node that independently communicates with the "boot node" and controls the smart contract life span on that node. When an election is created by the election administrator, a ballot smart contract is issued and installed on the appropriate district node. Every single related district node is granted permission to communicate with its own corresponding contract when the smart ballot contracts are formed. The vote information is validated by most of the associated district nodes when each voter casts a vote from their corresponding smart contract and each vote that they concur upon is added to the blockchain.

(ii). Boot Node:

Each institution runs a boot node that has authorized access to the network. A boot node is a coordination and discovery service that aids with district node discovery and communication. In order to let district nodes, locate their neighbors more quickly, the boot node operates on a static IP and does not maintain any state on the blockchain.

After building a safe and private blockchain, a further goal is to write and implement a smart contract that replicates the electronic voting procedure on the blockchain architecture.

B. Election based on a Smart Contract

A Smart Contract is defined following steps: (1) identifying the roles engaged in the agreement (in our example, the election agreement); (2) defining the agreement process (i.e., the election process); and (3) defining the transactions utilized in the smart contract (i.e., the voting transaction).

The parties required to take part in the contract are listed under the roles in a smart contract.
The following responsibilities are involved in elections:

(i). Election_administrator: To oversee the whole electoral process. Several reputable organizations and businesses could be included in this function. The election administrators designate permission nodes, register voters, choose the election's duration, and create the election.

(ii). Voter: A person who is legally entitled to cast a ballot. Voters can register, load their ballots, cast their votes, and then check their votes after the election is over.

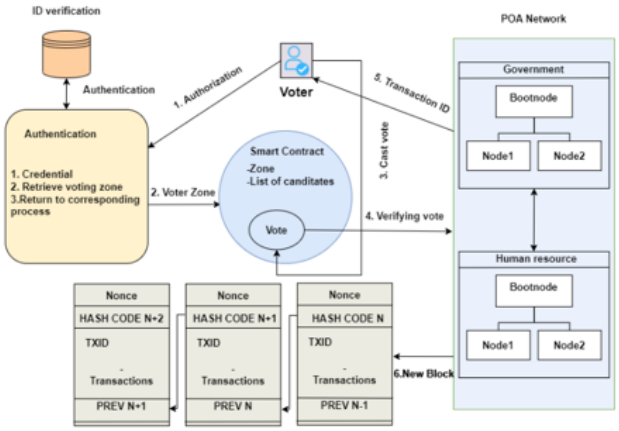

Fig 2: The Flow Diagram of Voting Processes

C. Election Process:

In our approach, each election system is illustrated by a collection of smart contracts that the election administrators put on the blockchain as shown in fig 1. Each voting district has a specified smart contract. The primary election-related activities are as follows:

(i). Election Creation: Election administrators use smart contracts to produce election ballots, including a list of potential voters for each district. Once the smart contracts are published on the blockchain, district nodes have access to them and may communicate with them.

(ii). Voter Registration: Voter registration is under the control of the election administration. When they create an election, the election administrators must supply a consistent list of eligible voters. In our approach, a matching identification wallet would be established for each qualified voter. For each election in which a voter is entitled to cast a ballot, an individual wallet is created.

(iii). Tallying Results: In smart contracts, the election results are calculated instantly. Each voting smart contract keeps track of the results for its respective location in its own memory.

(iv). Verifying Votes: Each voter obtains a transaction ID for his vote during the voting process. Voters may thus check that their votes were listed and counted accurately by viewing their votes on the blockchain. While prohibiting vote tracing, this kind of verification meets the standards for transparency.

Algorithm: Blockchain-Enabled E-Voting

Step 1: Voter 'A' submits A (Id + Fingerprint) for verification to the databases.

Step 2:

If A ∈ Voterlist HasNotBeenSubmit(A) == true

return the key and go to step 3.

Else, return False and abort.

Step 3: Send EVM the created key.

Step 4:

If ReceivedKey() == true do

Unlock the User Interface of EVM & join the

blockchain community. Move to step 5.

Else recheck.

Endif

Step 5: Use a secret key that only you know to cast your ballot. The hash (private key + nonce) depicts the voter in the blockchain ledger. The voting results will be kept in this hash.

Step 6: Connect the blockchain peer-to-peer connection to the present voting ledger.

Step 7: Maintain blockchain integrity by comparing the network's current root hash with the Merkel tree's root hash whenever a new block is produced.

D. Voting Transactions:

Each voter engages with a smart contract for the ballot that corresponds to her voting district. The district node that corresponds to this smart contract communicates with the blockchain and adds the vote to it. The transaction ID for each voter's vote is given to them individually for verification reasons. Each vote that has the support of most of the district nodes in question is recorded as an operation and added to the blockchain. This procedure is illustrated in Fig 2.

Therefore, in our system, a vote transaction provides no details. on the specific voter who casts a certain vote.

V. PERFORMANCE EVALUATION

The front-end application for this voting system is a web-based software program that is used in a controlled environment. We used several technologies for different purposes in implementing this application, such as ReactJs for the front end, NodeJs for backend services, and Metamask and Solidity to connect to this blockchain-based application. We have also used some other technologies like SQL, Ganache, Javascript, etc. Here is a brief description of these technologies.

A. Environmental setup

The testing environment consists of both a hardware and software environment. It consists of test terminals, test hardware setup, operating system settings, software configuration, and other test support. Javascript and Solidity are used as programming languages that are very popular these days and are widely used. In the database management system., MySQL has been used. The requirements in terms of hardware include a processor of 3.5GHZ and RAM of 8GB [19].

B. Results

Blockchain technology often enables users to check that their votes are appropriately recorded and tallied without endangering their privacy. Furthermore, anyone could be able to verify the counting without impairing confidentiality.

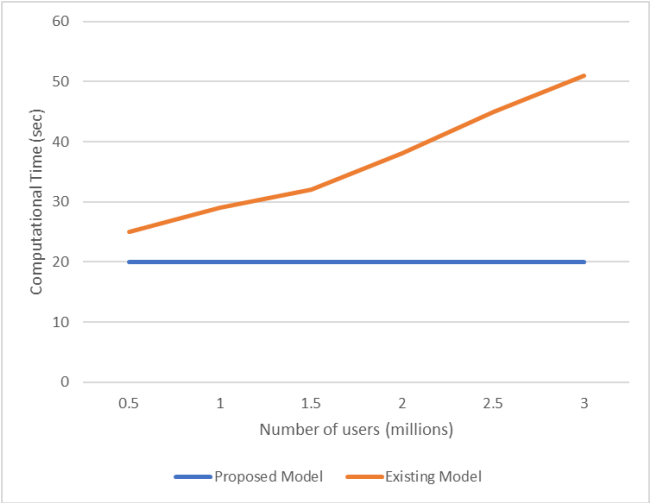

Fig 3: Computational Time (Existing System vs Proposed System)

Fig 4, states that the Computational Time of the Blockchain-based voting system is independent of the number of users. whereas the existing system takes a large time for a huge number of users.

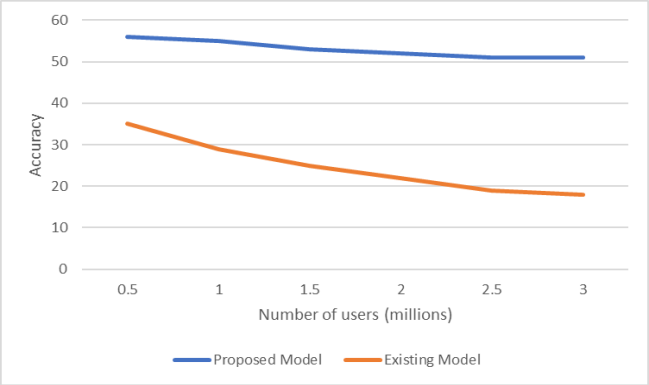

Fig. 4. Variation in Accuracy (Existing System vs Proposed System)

According to Fig. 5, the number of users directly affects how accurate the Blockchain-based voting system is, thus as the user base grows, so does the process' accuracy.

C. Discussion

The outcome is then displayed on the result screen. Comparing smart contracts to traditional written contracts, economic, increased efficiency, and risk depletion are three major advantages. Because smart contracts are easily verifiable and accessible to all blockchain users, they reinvent trust. The below table [2] displays the procedure for posting results. This table displays the total votes cast for each contender and the winner for various areas and seat numbers.

TABLE II. THE TOTAL VOTES CAST FOR EACH CONTENDER AND THE WINNER FOR VARIOUS AREAS AND SEAT NUMBERS

Region (Rg)	Seat No. (Sn)	Cand. of Party1	Cand. of Party2	Cand. of Party3	Winner
A1	1	4000	2000	500	Party1
A1	2	1000	5000	3000	Party2
A2	3	2000	1000	4000	Party3
A2	4	8000	6000	4000	Party1
		winner		Candidate of Party1	

The existing voting process invites several issues, including how trustworthy and transparent the system is, whether votes are altered before being counted, and how we can confirm the system's openness. Therefore, to address these types of problems, we looked into and proposed a web application employing blockchain technology via an Ethereum server by implementing smart contracts.

The next features [Table III] are likely the most well-known qualities of this technology that makes it appropriate for voting systems.

TABLE III. A COMPARISON OF VARIOUS VOTING SYSTEMS BASED ON THEIR FEATURES

Features	Traditional Voting System	E-voting System	Blockchain-based Electronic-Voting System
Time Consuming	✅	❌	❌
Secure Model	❌	❌	✅
Fewer Efforts	❌	✅	✅
Privacy Preservation	❌	❌	✅
More Efficient	❌	✅	✅
Trust on Third Party	✅	✅	❌
Process Overhead	✅	❌	❌
Votes Transparency	❌	❌	✅
Accurate Votes Counting	❌	✅	✅
Votes Tempering	✅	✅	✅
Trustworthy System	❌	❌	✅
Immutability & Verifiability	❌	❌	✅

Each vote forms a block after casting a ballot, adding to the chain. Since there is no chance of vote tampering or manipulation, the vote will be immediately counted when it is entered.

VI. CONCLUSION AND FUTURE DIRECTIONS

Since the 1970s, electronic voting has been employed in a variety of contexts and has a number of advantages over document systems, including more efficiency and lower error rates. However, when we utilize online voting systems, several concerns, such as security, transparency, and traceability, arise. To address these issues, blockchain is the ideal alternative. The blockchain-based voting system makes it possible for a more open kind of democracy where voters must express their opinions on particular bills and models. In this paper, we analyzed and discussed a blockchain-based e-voting system that uses smart contracts to facilitate safe and cost-effective elections with protecting voters' security. The recommended voting system has been built with Multichain, and a thorough analysis shows that it effectively satisfies key requirements for an electronic voting scheme.

As future work, more implementation or changes can be made to improve its performance and make it suitable for use in national voting systems. A facial recognition and fingerprint module can be added to this system to improve its security.

REFERENCES

1. P. Shen et al., "A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology," IEEE Conference, 2022.
2. Singhal, B., Dhameja, G., Panda, P.S.: How blockchain works, in: Beginning Blockchain, Springer, 2018, pp. 31-148.
3. M. Sober et al., "A Voting-Based Blockchain Interoperability Oracle," IEEE Conference, 2021.
4. V. Vijeya Kaveri, V. Meenakshi, A. S, A. P, and K. B, "Blockchain-based Reliable Electronic Voting Technology," 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022, pp. 1713-1717.
5. https://www.ethos.io/cryptocurrency-news-ethos-blog. Accessed: 2020-01-27.
6. K. L. Ohammah, S. Thomas, A. Obadiah, S. Mohammed, and Y. S. Lolo, "A Survey on Electronic Voting On Blockchain," IEEE Conference, 2022, pp. 1-4.
7. https://trufflesuite.com/docs/truffle/reference/configuration/.
8. Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7:24477–24488, 2019.
9. Jangada, N. Dadlani, S. Raina, V. Sooraj and A. R. Buchade, "De-Centralized Voting System using Blockchain," IEEE Conference, 2022, pp. 1-5.
10. A. H. Othman et al., "Online Voting System Based on IoT and Ethereum Blockchain," International Conference of Technology, Science and Administration (ICTSA), 2021.
11. Bulut, Rumeysa, et al. "Blockchain-based electronic voting system for elections in Turkey." IEEE Conference, 2019.
12. M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in 2022 IEEE Access, vol. 10, pp. 59958-59969, 2022.
13. Neelam Chauhan, Rajendra Kumar Dwivedi, "A Survey on Designing A Secure Smart Healthcare System with Blockchain", Part of the LNDECT Book Series, Springer, 3rd Springer International Conference on Mobile Computing and Sustainable Informatics (ICMCSI 2022), Tribhuvan University, Nepal, 27-28 Jan 2022.
14. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
15. H. -T. et al., "A Blockchain-Based Network Security Mechanism for Voting Systems," 1st International Cognitive Cities Conference (IC3), 2018, pp. 227-230.
16. Hamdan, Yasir Babiker, and A. Sathesh. "Construction of Efficient Smart Voting Machine with Liveness Detection Module." Journal of Innovative Image Processing (JIIP) 3, no. 03 (2021): 255-268.
17. Ayyasamy, S. "Metadata Securing Approach on Ubiquitous Computing Devices with an Optimized Blockchain Model." Journal of Ubiquitous Computing and Communication Technologies 4, no. 2 (2022): 57-67.
18. https://www.ibm.com/uk-en/blockchain
19. https://ethereum.org/en/developers/
20. https://www.coindesk.com/learn/how-does-blockchain-technology-work/
21. Atul Lal Shrivastava, Rajendra Kumar Dwivedi, "Designing A Secure Vehicular Internet of Things (IoT) using Blockchain: A Review",1st IEEE International Conference on Advances in Computing and Future Communication Technologies (ICACFCT 2021), MIET Meerut, India, 16-17 Dec, 2021 (2021).