IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12225

ELECTRONIC VOTING OR E-VOTING SYSTEM USING BLOCKCHAIN AND DEEPLEARNING

Prof. Manjunatha T N[1],

Manoj C[2], Raghu S[3], Parth G Nair[4], Lokesh Kumar S[5]

Assistant Professor, Computer Science, East West Institute of Technology, Bangalore, India [1]

Student, Computer Science, East West Institute of Technology, Bangalore, India[2-5]

Abstract: Electronic voting or e-voting, has been used in various forms from the 90s. Increase efficiency and reduce errors. However, wide adoption of such systems remains a challenge, especially in terms of improving resilience to potential failures. Blockchain is today's disruptive technology and promises to improve universal flexibility of electronic polling systems. It represents an attempt to exploit the advantages of blockchain for security. The proposed system fulfills the basic requirements of electronic voting systems and achieves persistent verifiability. This wrapper describes the details about proposed electronic voting system and its fulfilment using a multi-chain manifesto. This paper contains a detailed estimation of the system and it demonstrates successfully about the effectiveness in achieving an ongoing auditable electronic voting system.

Keywords: Cryptography, peer-to-peer, deep learning, security, distributed ledger technology, EVM.

I. INTRODUCTION

Elections are the cornerstone of democratic systems that allow ordinary citizens to convey their opinions in the form of the ballots. As important to community, electoral process must be clear and trustworthy to guarantee the trust of the participants. In this circumstances, selection approaches are a constantly evolving field. This development is regarding to the make the system secure, auditable, and transluscent. given that Importantly, perpetual efforts must be made to enhance the overall ability and persistence of the electoral system. Electronic voting system plays an important part here. Already their prior used as punch voting in the earlier 1960's, electronic voting systems have made remarkable progress in adapting to Internet technology (Gobel and team., 2015).

Therefore, in order to promote their widespread use, e-voting systems must adhere to a set of benchmark requirements. These criteria include non-repudiation, vote fairness, including voter confidentiality, among others. One of the cutting-edge technologies, blockchain has a solid cryptographic basis that enables apps to take advantage of these capabilities to provide security management solutions. The transactions that take place during the formation of a blockchain are managed and shared in the same way that data structures are. It functions primarily as a decentralised database that keeps an exhaustive list of datasets that are continually sprouting and expanding while being guarded against unwanted modification, tampering, and tampering. Any user may join to a blockchain, post new transactions to the network, approve transactions, and add new blocks.

Every block is given a cryptographic hash that serves as the block's fingerprint and is valid as long as the data included in the block stays the same. Any modification to the block will immediately cause the cryptographic hash to alter, suggesting that the contents may have undergone a malicious change. Consequently, because of its solid basis in cryptography, Blockchain is being utilised more and more to reduce fraudulent transactions in many different industries. Vote confidentiality and voter anonymity are the main topics of our study, which also examines important problems like end-to-end validation. An effective voting system that preserves the integrity of the voting process is built on these difficulties. This white paper details our attempts to use blockchain technology to address these problems.

Our solution specifically employs the open-source blockchain platform Multichain (Multichain, 2017) as the foundation for system development and is based on the Voter method (Ryan, 2008). The system creates a robust cryptographic hash for each vote transaction based on voter-specific data to preserve the anonymity and integrity of votes.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12225

Additionally, this hash is transmitted to the voter through a secure channel. to improve verification quicker. As an outcome, this necessary aspects the prerequisites for an electronic voting system.

II. BLOCKCHAIN TECHNOLOGY

It might be confusing since different people/organizations refer to different things by the term "blockchain revolution." But, decentralized records are what it actually refers to. H. Transaction logs are disseminated among the network's nodes rather than kept on a single central server. Although blockchain technology has been there since the 1980s, Bitcoin's rise to prominence is the key factor driving its current popularity. In 2009, Bitcoin's program started. Despite the fact that many people now credit Bitcoin as the first real-world, paperless, digital money, due to the absence of centralized transaction management, this asset or currency has yet to reached broad acceptance. It could not have any worth. It was created using mathematics from the Blockchain.

A distributed system is one in which no one node within the linked network has full or exclusive power. A type of networked computer system in Internet-based IT systems is referred to as a distributed system. Elections, as you are aware, are crucial to a democratic system's smooth operation. Due to the development of internet technology, county operations and administration are now subject to a variety of outside influences. Making the voting process fair is so crucial and essential now more than ever. Dictatorships have plagued many nations in the past or present, constantly causing pain to common people.

The Constitution's promises of fundamental human rights and freedoms were denied to the common people. Given this context, a fair and rational election system is crucial for the correct expansion and advancement of the nation. Election-related technology, specifically H. EVMs, has been widely criticized in our nation, I H. India, for anomalies in reporting election results. There are many unanswered issues involving the underlying structure and design of the EVM, as well as how hacks and manipulation may be possible. There are numerous other ways that the current voting mechanism may be corrupted. The existing system has shown several instances of fraud, such as: All of this renders the election process improbable. Yet if the voting process is made more open and responsible, these issues with the existing democratic system may be fixed. H. Be more fair. Although the current approach does succeed in achieving voter anonymity, it is still not entirely transparent. After all, because the system is unreliable, voters are expected to have unquestioning faith in the outcome of elections. Nonetheless, there has recently been more support for the introduction of an internet-based voting system in the nation. I have produced a Programme.

III. DEEP LEARNING

Techniques for deep learning may use very huge face datasets to develop rich and compact representations of faces, which enables existing models to initially perform as well as, and then beyond, human face recognition abilities. Face recognition is a difficult matter and makes it hard to recognise or identify faces in photographs and films. Detection, alignment, feature extraction, and a recognition task are the steps in the process of face recognition. For facial recognition tests, deep learning models originally got near but then outperformed human performance.

IV. LITERATURE SURVEY

This introduces and discusses some research related to electronic voting systems based on blockchain technology, which can solve security and privacy issues in electronic voting systems.

[1] Its blockchain framework is Hyperledger Fabric. Consensus with Byzantine fault tolerance that is practical. Hyperledger Sawtooth can be used to further enhance the proposed method. allows for both the execution of transactions in parallel.

[2] Designate voting storage as an asset. in the safe. Usable and scalable. This proposed system uses a multi-chain blockchain network. This limits each voter to her one transaction. A Trusted Third Party (TTP) is used to verify the validity of voters using secret messages that voters send to TIP. The proposed system would consist of greater delays as the secret messages sent by each voter would have to be verified by her TIP and the Election Commission. A reference number is then generated that can be used to indicate and vote for the candidate.

[3] The proposed system is a smart m.mart contract on the .boot node. The recommended framework is Exonium. Quorum and Guess. Exonium is a production system that can be used with cryptocurrencies. Large scale implementations are expensive. if there are alternative equally powerful and free frameworks. The Ethereum-based frameworks Quorum and Gail do not permit transaction execution in parallel. Scalability and speed are still so limited. Hyperledger Sawroot can be used to further enrich the suggested system. allows for the transaction processing in parallel.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12225

[4] A generalized blockchain electronic voting system is proposed using her SHA encryption of voter information. Voting block information. It will be added to the selected candidate blockchain. Using a different chaun for each candidate has a lot of overhead. The system does not describe the implementation using any particular framework. The advantages of blockchain-based voting methods are highlighted.

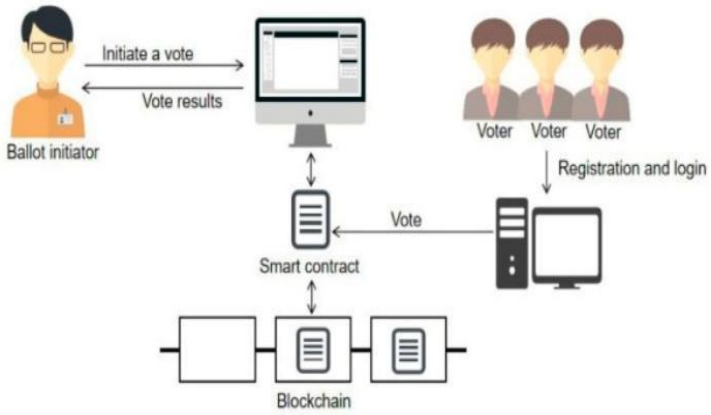
[5] The proposed system uses elliptic curve cryptography, where voters use their private keys to create signatures for their voting blocks, and the signatures use the voters' public keys residing in a public key infrastructure database. and validated. Even if the system proposes complex procedures for checking voice blocks, the PKI database used is still vulnerable. What to do if exposed You can disable the entire process.

V. EXISITING SYSTEM

The current method utilised to assist or handle the casting and counting of votes is known as an electronic voting machine (EVM). The Control unit and the Balloting unit are the two units that make up its design. The Control unit is positioned next to the poll worker, while the Balloting unit is positioned within the voting booth. Hackers may easily gain access to the current EVMs and manipulate the count numbers. Also, it has a touch-screen and is reasonably priced. The shortcomings include that it is susceptible to bad code, can be hacked, and can have votes tampered with. Numerous persons with physical disabilities have expressed their dissatisfaction with the efficiency and accuracy of touch-screen voting. And it results in the voter accidentally casting a ballot for someone. The EVMs might be equipped with fake display devices that would display modified figures. High humidity levels might harm equipment, which will lead to data loss.

VI. PROPOSED SYSTEM

In the proposed system, the voting mechanism is included in smart contracts that are written in the Solidity programming language. A smart contract is generated and then compiled using truffle to produce abi and bytecode. A contract cannot be altered after it has been created and made available on the blockchain. Web3.js, which gives access to the contract's variables and methods and communicates with the smart contract, may be used to access built contract.



Election candidates can be added using the admin login. Using the registration procedure on the internet, voters can register. Only users with legitimate credentials are allowed to participate in elections, and administrators can check the registration information of users. Every time a user casts a vote, a new block on the blockchain is created with the results. So, every vote has a blockchain transaction associated with it. The aforementioned transactions will be completed using a Metamask account. The length of elections may be chosen by the Administrator. While a vote is being cast for a candidate on the portal, a voter may only do so once. The administrator can view the election results and the essential information when the stipulated time has gone.

VII. CONCLUSION

Blockchain transparency allows for additional audits and insights into elections. These attributes are perpendicular to some of the needs of a legal system. These characteristics come from redistributive networks and can bring additional democratic processes to elections, especially direct election systems. To make electronic voting more open, transparent, and testable, one possible answer is based on blockchain technology. This article explores the potential of blockchain technology and its qualities in the topic of electronic voting.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12225

The blockchain will be publicly verifiable and distributed in such a way that no one can tamper with it. The idea of adapting digital selection systems to make mass-market voting cheaper, faster and easier could be appealing in a wired society. created a cheap and fast method of voting, standardized it in the eyes of the voters, removed the obvious power barrier between voters and officials, and put obvious pressure on officials. It also opens the door to another form of direct democracy, allowing voters to determine their power over bills and proposals.

REFERENCES

[1.]Yu and Paul. “Hyperledger fabric with practical Byzantine Fault Tolerance” (2018): 01-09.
[2.] Ganji, Raghavendra, and B. N. Yatish. ”ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN.” (2018).
[3.]Yi, Haibo. ”Securing e-voting based on blockchain in P2P network.” EURASIP Journal on Wireless Communications and Networking 2019, no. 1 (2019): 137.
[4.]Hjalmarsson and team. “ELECTION AS A SMART CONTRACT.” (JULY 2018).
[5.]Patil and other. “GENERAL EXPLANATION OF BLOCKCHAIN BASED VOTING SYSTEMS.”(IRJET.Nov 2018).
[6.]Ayed, Ahmed Ben. ”A conceptual secure blockchain-based electronic voting system.” International Journal of Network Security & Its Applications 9, no. 3 (2017): 01-09.
[7.]”What is a Digital Signature? - Definition from WhatIs.com.” SearchSecurity. Accessed September 11,(2019). https://searchsecurity.techtarget.com/definition/digital-signature
[8.]Sitoh, Paul. ”What Are the Differences Between Ethereum, Hyperledger Fabric and Hyperledger Sawtooth?” Medium. Last modified February 14, (2019).
[9.] ”Introduction - Sawtooth V1.0.5 Documentation.” Hyperledger Sawtooth. Access On September 11, (2019).
[10.]Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. ”Large Scale election based on blockchain.” Procedia Computer Science 129, (2018).

