International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

Blockchain Based E-Voting System

Praful M. Kukwase, Gauri P. Kolte, Ashwini D. Sawarkar , Chaitali K. Rajput, Prof. Jiwan Dehankar

Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur.

Abstract :-

For a long time, creating an electronic voting system that meets legislators' legal criteria has been a struggle. Distributed ledger technology (DLT) is a cutting-edge innovation. breakthrough in the field of information technology Blockchain technologies have an unlimited number of applications that can profit from them. economy based on sharing The purpose of this study is to assess the application. blockchain as a service for implementing distributed electronic transactions Electoral systems The paper elicits the needs of the construction industry. electronic voting systems, as well as the legal and technological issues that surround them. the drawbacks of adopting blockchain as a service for achieving such goals systems. The study begins by assessing some of the most popular Frameworks for delivering blockchain as a service. We Then, based on blockchain, offer a unique electronic voting mechanism. that takes care of all the flaws we found.

Introduction

Election security is a concern of national security in any democracy. For a decade, the computer security sector has explored the potential of electronic voting systems with the goal of reducing the cost of holding a national election while maintaining and improving election security. The voting procedure has been based on pen and paper since the beginning of democratically electing candidates. To reduce fraud and have the voting process traceable and verifiable, it is important to replace the existing pen and paper method with a modern election system

As a decentralised database, blockchain offers new tools for developing trustless and decentralised systems. There is no centralised trustworthy coordinator in the blockchain system. Instead, each node in the blockchain system stores the data block independently on its own computer. A decentralised and open-membership peerto-peer network maintains the blockchain. Initially, this technology was created for money transfers. Researchers are attempting to repurpose Blockchain in various areas of research, such as coordinating the Internet of Things, carbon dating, and health-care. This spurred the creation of Ethereum, which is widely regarded as a watershed moment in the development of blockchain technology. It has a Turing complete programming language, and users can utilise the Ethereum network's smart contract to do the function.

For the voting mechanism, blockchain might be used as a trusted public bulletin board. Furthermore, the blockchain smart contract functioned as a trusted computer whose output is publicly trusted. However, just substituting blockchain for the bulletin board is not a good idea. This might be seen in because there will be too many transactions for voters to detect and blockchain computation is extremely difficult. In this work, we propose a blockchain-based decentralised trustless evoting system. The computation is based on a decentralised blockchain in a decentralised system. The trustless approach means that voters do not have to rely on the election administrator; instead, all voters share the same level of trust. The system's correctness is determined by the entire protocol.

The security community has seen electronic voting machines as flawed, especially due to physical security issues. Anyone with physical access to such a machine has the ability to sabotage it, affecting all votes cast on that machine. This is where blockchain technology comes in. A blockchain is a public ledger that is distributed, immutable, and indisputable. The four primary elements of this innovative technology are as follows:

(I) The ledger can be found in a variety of places: There is no single point of failure in the distributed ledger's upkeep.

(ii)The ability to append new transactions to the ledger is disseminated.

(iii) Any proposed "new block" to the ledger must refer to the previous version of the ledger, forming an immutable chain that gives the blockchain its name and prohibits interference with the integrity of the ledger.

Literature Survey

Authentication of voters: Authentication of voters can be accomplished in a variety of ways. Voter authentication, according to Kriti Patidar and Dr. Jain, can be done using private key cryptography, which must be delivered to voters prior to the voting process. Some authority should register voters, and while registering voters, keys must be generated and distributed to voters on hand. Cosmas Krisna Adiputra proposes a public-private key infrastructure, in which the electoral commission (or another election manager) generates a key-pair for the election (PE; SE), which is then used to encrypt and decrypt voter messages. After that, each voter must

create their own key pair. The key is denoted by (PV X; SV X). voters must register their public key pv x with the electoral commission using a valid id to be eligible to vote. after that, the electoral commission validates each voter's identification and registers them. a public list corresponding to pv x's public key; or if the voter is ineligible, the ballot is rejected. it is critical to in this approach, each voter's public key is kept confidential. only the controlling body receives it.

fririk has a unique perspective on things hjálmarsson intends to utilise a six-digit pin for voter identification.that a voter can use to verify their identity the individual is recognised and verified by the system by providing an auokenni electronic id in the voting booth, and the 6-digit pin that corresponds in the absence of oversight

Verifying voter identity from diverse perspectives is always a challenge; some studies have used biometric methods, such as face comparison, fingerprint, Iris, and retinal scan, but these can be skewed and easily manipulated or stolen. However, we believe that utilising complicated algorithms that are difficult to crack is one method to protect the stolen biometrics data. Instead of preserving the biometric information as binary data and then storing it as a reference string, it can be hashed using any hashing technique. During the validation and identification process, the sample model should be converted to a hash value and then compared to the reference value.

Problem statement

Our goal is to use blockchain technology to tackle the problems associated with digital voting. Voter fraud could be reduced and voter access increased with blockchain-enabled e-voting.

Objectives

As a result, the voting mechanism proposed here must meet the following criteria:

1)The election system must be transparent and open to public scrutiny.

2)The election system must ensure that the voter's vote is properly recorded.

3)Only eligible voters should be permitted to cast ballots.

4)The election system should be impenetrable to tampering.

5)No power-hungry organisation should be able to rig and manipulate the election process.

The most important prerequisites are met while using a Blockchain:

Authentication: Voting will be restricted to registered voters only.

Anonymity: The technology precludes any collusion between the votes cast by the participants.

Proposed System

A 'chain' of blocks could be used as a simple rationalisation. A block is a large collection of information. Mining is a technique that collects and organises information so that it can be used in a very specific way. Using a scientific hash, each block may be identified (also referred to as a digital fingerprint). Because the shaped block can contain a hash of the previous block, blocks will form a sequence starting with the first block ever (known as the Genesis Block) and ending with the shaped block. During this procedure, all of the data can be linked together using a connected list structure.

Methodology

1) Organizing elections:

Election administrators are in charge of organising elections. Using a decentralised app to cast ballots (dApp). This decade has been a difficult one for me. An election creation smart interacts with a tralized app.contract, in which the administrator establishes a list of permissible options didates and voting districts are two things that come to mind while thinking about voting districts. This smart contract gives rise to a set of smart contracts for voting and deploys them on the blockchain For each voting, a blockchain with a list of candidates is used.district, with each voting district serving as a parameter each smart contract for each ballot As soon as the election is set up, Permission is granted to each appropriate district node to connect with his appropriate smart contract for voting.

2) Registration of voters:

The election administrators are in charge of the voter registration process. Election administrators must define a deterministic list of eligible voters when creating an election. This necessitates the creation of a government identity verification service that can securely authenticate and authorise qualified people. Each of the eligible individuals might use such services to verify their eligibility. A voter should have a digital ID and a PIN number. information on the voting district in which the voter resides. A comparable wallet would be created for each qualified voter. The wallet generated for each individual voter should be unique for each election for which the voter is eligible, and an NIZKP could be used to

establish such a wallet so that the system does not know which wallet matches which voter.

3) Transaction of a vote:

When a person casts a vote in a poll, The voter interacts with a smart contract on the ballot in their district. with the same voting district as any other election each and every voter This smart contract communicates with the Ethernium blockchain. Blockchain via the district node that corresponds to it, which If a consensus is established, the vote is sent to the blockchain. between the majority of the nodes in the corresponding district Each vote is recorded on the blockchain as a transaction. whereas the transaction is received by each individual voter For the purpose of authenticating their vote, they must provide identification (see "Verifying Your Vote"). section "vote"). On the blockchain, each transaction contains information. details on who was voted for and where they voted of the aforesaid vote Each vote is added to the total. If a blockchain is linked to a smart contract for voting, and then only.

4) Compiling the results:

The election results are tallied in real time by smart contracts. Each ballot has a smart contract. does their own tally for their assigned spot in It has its own storage. When an election is completed, the final result is announced. Each smart contract is made public.

5) Vote verification:

As previously stated, each individual is unique. The voter receives his vote's transaction ID. Each individual voters can go to their local government official and express their concerns. after authenticating oneself, present their transaction ID utilising his electronic ID and the PIN that goes with it The Using district node access to the internet, a government official The blockchain explorer is used to locate the blockchain. transaction on the database with the corresponding transaction ID blockchain. As a result, the voter may see his vote on the blockchain.

Conclusion & Future Work

Since the 1970s, electronic voting has been utilised in many forms, with key advantages over paper-based systems such as enhanced efficiency and lower error rates. With the explosive expansion of blockchain technology, a number of efforts have been launched to investigate the potential of using blockchain to facilitate an effective e-voting solution. This paper describes one such endeavour that takes advantage of blockchain's cryptographic foundations and transparency to create an effective e-voting solution. Multichain has been used to achieve the proposed method. An in-depth analysis of the technique reveals that it is effective in meeting the fundamental conditions for an e-voting scheme. We are continuing to work on enhancing the resistance of blockchain technology to attacks. For e-voting systems, there will be a 'double spending' problem, which will translate to 'double voting.' Although The detection of changeable changes in a transaction is a key success for blockchain technology. However, successful demonstrations of such phenomena have been made, prompting us to look into it more farther. To this end, we argue that an effective paradigm for establishing reliable provenance for electronic voting exists. To develop an end-to-end verifiable e-voting strategy, systems will be critical. It will take a lot of effort to do this. An extra provenance layer is being developed to help the existing blockchain-based system infrastructure.

References

1) Friðrik Þ. Hjálmarsson, Gunnlaugur 0K. Hreiðarsson ,(2019) “BlockchainBased E-Voting System” ,

2) Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde(2021) “Blockchain-Based E-Voting System”.

3) Agora (2017). Agora: Bringing our voting systems into the 21st century

4) Kirill Nikitin, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nico- las Gailly, Ismail Khoffi, Justin Cappos and Bryan Ford (2017). CHAINIAC: Proactive SoftwareUpdate Transparency via Collectively Signed Skipchains and Verified Builds.

5) Alin Tomescu and Srinivas Devadas(2017). Catena: Efficient Nonequivocation via Bitcoin .

6) Michael del Castillo (2018). Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote.

7) Ethereum Blog. (2018). On Public and Private Blockchains Ethereum Blog.

8) Xiao S., Wang X.A., Wang W., Wang H. (2020) Survey on Blockchain-Based Electronic Voting. In: Barolli L., Nishino H., Miwa H. (eds) Advances in Intelligent Networking and Collaborative Systems. INCoS 2019. Advances in Intelligent Systems and Computing, vol 1035. Springer, Cham.

9) Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. IEEE Transactions on Dependable and Secure Computing.

10) K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019.