RESEARCH ARTICLE OPEN ACCESS

Online Voting System Using Blockchain Technology

Farzana Khareem [1], Muhammad Safeer [2], Nadhiya Shafeeq [3], Shanavas KS [4] L i j a Joy [5]

Department of Computer Science and Engineering,
KMEA Engineering College, Kerala - India

ABSTRACT

In today's world, online voting is becoming more popular. It has a lot of potential for lowering administrative expenses and increasing voter turnout. It eliminates the need for voters to travel topolling locations or print ballot papers because they can vote fromanywhere with anInternet connection. Despite these advantages, online voting methods are viewed with scepticism since they poseadditional risks. A single flaw has thepotential to lead to large-scale vote tampering. When utilized in elections, electronic voting systems must be legitimate, accurate, safe, and convenient.

However, inherent difficulties connected with electronic voting methods may limit adoption. Blockchain technology was created to address these concerns and provides decentralized nodesfor electronic voting. It is utilized to create electronic voting systems primarily due to its end-to-end verification benefits. With dispersed,non-repudiation, and security protection features, this technology is a lovely replacement for traditional electronic voting solutions.

***Keywords**: - Blockchain, Hashing, Authentication, SHA, SHA-256.*

I. INTRODUCTION

In today's world, online voting is becoming more popular. It has a lot of potential for lowering administrative expenses and increasing voter turnout. It eliminates the need for voters to travel to polling locations or print ballot papers because they can vote from anywhere with an Internet connection.Despite these advantages, online voting methods are viewed with scepticism since they pose additional risks. A single flaw has the potential to lead to large-scale vote tampering. When utilized in elections, electronic voting systems must be legitimate, accurate, safe, and convenient.

However, the potential for difficulties with computerized voting methods may limit acceptance. Blockchain technology was created to address these concerns and provides decentralized nodes for electronic voting. It is utilised to create electronic voting systems primarily due to its end-to-end verification benefits.With dispersed,non-repudiation, and security protection features, this technology is a lovely replacement for traditional electronic voting solutions.

Many developing countries rely on democracy to keep power in the hands of the people, who choose their government through elections. In elections, polling officials and polling stations

are critical. From the year of independencetill today, many changes have occurred in election procedures; first, ballotpapers were used as a voting medium, and later, electronic voting machines were introduced, with voters selecting from a list of buttons, each representing a symbol.Many efforts have been implemented throughout time to lower the expenses of election operations without jeopardizing voters' privacy or failing to follow constitutional rules, yet there are still many incidents highlighting the lack of effective voter authentication methods. Using multifactor biometric scanning and blockchain technology, options for guaranteeing voter authentication and privacy are available.[7]

The traditional or paper-based polling method increased people's trust in the majority voting selection.It has aided in the democratization of the democratic process and electoral system for electing constituencies and governments.

In 2018,out of almost 200 countries, 167 have democracy, with the others being either completely flawed or hybrid. Since the commencement of the voting system, the secret voting model has been utilised to increase trust in democratic institutions.

For online or electronic voting, blockchain technology provides a decentralized node. Because of their end-to-end verification advantages, distributed ledger technologies such as blockchain have recently been employed to create electronic voting systems. With advantages like decentralization, non- repudiation, and security protection, blockchain is a compelling alternative to traditional electronic voting systems.It can be used for both private and publicvoting.

II. LITERATURE SURVEY

Because the security of electronic voting is the most important feature in practical applications, researchers in many countries are payingincreasing attention to the privacy

protection in the electronic voting protocol. The security requirements for electronic voting were defined by Japanese academicians Fujioka, Okamoto, and Ohta[10].At the same time, they proposed the well-known FOO electronic voting procedure (FOO stands for the authors' initials). Many well-known electronic voting systems, such as the Sensus system at the University of Washington and the EVOX system at the Massachusetts Institute of Technology , are based on this technique. The Sensus system is a real-worldelectronic voting system based on the FOO protocol developed by University of Washington researchers.It complies with the FOO protocol's security criteria. This approach can secure voters' privacy even if electoral institutions conspire withone another.Voters can check to see if their votes were appropriately counted. They can question the accuracy of the election results anonymously if their votes are not counted correctly. The FOO protocol is also used in the EVOX system developed by MIT researchers. The preparation stage, authorisation stage, anonymization stage,collecting stage, and vote-counting stage are all required to complete the electronic voting process. The anonymity of voters is also substantially enhanced by this voting mechanism.

Aside from standard electronic voting, some newer voting systems are increasingly incorporating blockchain technology. Research on user privacy and security is also a major topic in the voting system based on blockchain technology[5]. It created an electronic voting system based on the Bitcoin blockchain that allows candidates to vote while ensuring individual voting privacy. The low scalability of this method is a negative.

The efficiency of the voting process can be improved by creating a voting smart contract on the blockchain, and the voting contract can be utilised in different directions.Through third- party solutions, smart contracts make voting easier. Na et al. proposed a blockchain-based chat system in which users can vote, with the system ensuring the anonymity of the users' voting and chatting processes. Each user is only permitted to vote weighted once under the

voting process developed by Kshetri et al. Despite the fact that this strategy can just prevent users from voting maliciously within the system, users who want to vote maliciously can always create several user accounts. According to a survey in , the number of smart contracts implemented on the Ethereum platform has been the biggest among other blockchain voting systems since 2018.Yavuz et al. built a voting programme for Android using the Ethereum platform, however its functions were too basic. There are various real application scenarios of the voting system in different blockchain platforms, such as a streamlined voting technique of Quantum blockchain .

Zhang et al. suggested a voting method on the Hyperledger platform that ensures user privacy. This method can detect and rectify ballots, but it cannot ensure that the ballots are fair . On the blockchain, there are numerous voting systems that are designed to protect the privacy of voting users.

III. METHODOLOGY

A blockchain is a growing collection of blocks with cryptographic connections that began as a chain of blocks. Each block contains the preceding block's hash, timestamp, and transaction data. The blockchain was built with data security in mind. Voting is a new phase of blockchain technology, and academics are attempting to capitalise on characteristics like transparency, secrecy, and non-repudiation, which are critical for voting applications. Researchers are attempting to utilize benefits such as transparency, secrecy, and non- repudiation that are crucial for voting applications [4] with the use of blockchain for electronic voting applications. Efforts to use blockchain technology to protect and remedy elections have recently gained a lot ofattention, thanks to the use of blockchain for electronic voting apps.[6]

Blockchain

Blockchain for electronic voting applications, as well as efforts to use blockchain technology to safeguard and

correct elections, have recently gotten a lot of attention.The rest of the paper is laid out as follows, explains how blockchain technology works and provides a comprehensive background on the concept. It is discussed how blockchain technology can be used to transfer the electronic voting system. The challenges of establishing online voting systems are identified, as well as their solutions. The use of biometric authentication.

Blockchain Technology can be characterized as a method of storing data in such a way that it is impossible, or at the very least difficult[1], to deceive the system. A blockchain is a digital ledger that is shared across a whole network of computers. A transaction can be found in everyblock of the blockchain. When a new transaction is seen in the blockchain, a record or copy of it is added to each user's ledger. A blockchain can alsobe thought of as a database variant. When a block is added to the blockchain, changing its contents becomes an inconvenient operation unless the majority of blockchain users agree to do so, because each block has its unique hash value and timestamp. These hash codes or values are created by converting digital data

into a string of integers and alphabets using a mathematical function or algorithm. The hash code or hash value changes erratically if any information on the blockchain is changed or altered in any way. In this way, it provides security because a hacker can disrupt the block chain without understanding what it means. Because the data inside the blockchain is encrypted using the hashing algorithm, blockchain networks are known as the most secure. It is also a decentralized network, which implies that the nodes in the blockchain are spread in such a way that exploiting the nodes is difficult. This is one of the most significant factors to consider when choosing a blockchain for security.[8]

Hashing

Hashing is a technique for converting a variable and arbitrary input size to a set output size. There are numerous functions available.which do various hashing levels SHA-256 has been used to provide security.SHA-256 is a

cryptographic hash algorithm.SHA-1 (also known as SHA-2) is a successor hash algorithm.It is one of the most powerful hash functions accessible.The SHA-256 algorithm is not substantially more complicated to code than the SHA-1 algorithm.is not yet tainted in any manner. AES uses a 256-bit key.Symmetric key encryption is an excellent partner feature.Cypher, which means that the same key is used for encryption and decryption.encryption and decryption In contrast to its forerunners, the algorithm's its versatility comes from the fact that it accepts any input length and produces but all other methods have a fixed output length.

MD5 algorithm

The MD5 algorithm is frequently used for hashing and produces a 128-nit or 32-character hash result. MD5 isthe most recent algorithm in the sequence, with Md2 before it. MD3 and MD4 were also known. The algorithm was created by It was designed to be used as a cryptographic hashing technique, but it wasn't.has some issues that limit the manufacturing of unique items .As a result, it is vulnerable to some attacks. RIPEMD stands for Race Integrity Primitive Evaluation Message Digest. Hans Dobbertin invented a family of hash functions.the year 1996 This method was created to take the role of MD5.solution that is more secure It has a few different versions.RIPEMD-128, RIPEMD-160, and others have emerged throughout time.RIPEMD256 and RIPEMD-320 are two RIPEMD variants.[5]

Another cryptographic hash algorithm is SHA (Secure Hashing Algorithm), which produces a 160-bit hash result with 40 hexadecimal characters. The algorithm was unable to withstand collusion assaults, and its use began to diminish after 2005. SHA 3 and SHA 256 aretwo new algorithms that have been proposed during this time. The US National Security Agency created the SHA 2 algorithm set. SHA 256 and SHA 512 are new hash algorithms that have no collusion issues and are considered secure otherwise, at least for the time

being..Guido Bertoni, Joan Daemen, and Michael Peeters created the Keccak family of algorithms.In contrast to its counterparts, the method is flexible in that it accepts any length of input and produces an arbitrary length of output, whereas all other algorithms create a set length output.

Blockchain technology can be characterized as a method of storing data in such a way that it is impossible, or at the very least difficult, to trick the system. A blockchain is a digital ledger that is shared across a whole network of computers. A transaction can be found in every block of the blockchain.[3] When a new transaction is seen in the blockchain, a record or copy of it is added to each user's ledger.A blockchain can also be thought of as a database variant. When a block is added to the blockchain, changing its contents becomes an inconvenient operation unless the majority of blockchain users agree to do so, because each block has its unique hash value and timestamp.These hash codes or values are created by converting digital data into a string of integers and alphabets using a mathematical function or algorithm. The hash code or hash value changes erratically if any information on the blockchain is changed or altered in any way. In this way, it provides security because a hacker can disrupt the block chain without understanding what it means.Because the data inside the blockchain is encrypted using the hashing algorithm, blockchain networks are known as the most secure.It is also a decentralized network, which implies that the nodes in the blockchain are spread in such a way that exploiting the nodes is difficult.This is one of the most significant factors to consider when choosing a blockchain for security.[2]

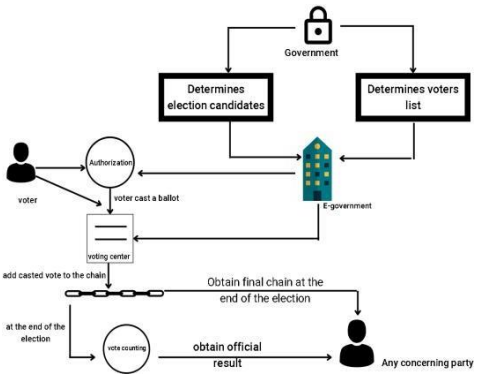

Fig 3.1. Blockchain voting systems architectural overview.

Candidate Registration:

The account calling the smart contract must not be admin. This is the initial registration criterionto check for candidate registration. Only if the preceding conditions are met does the procedure continue.

The condition is correct. Only the administrator has the ability to add a candidate. Candidate has ID and name parameters, where ID is a unique identifier.parameter and name aren't the same thing.

Voter Registration:

The name and address of the voter are required for voter registration. The voter list is kept private. Every time a voter is added, the variable 'voters count' is incremented. The variable 'voted' is set when registering for the first time. as an initial value of 'false' The variable'registered' has been assigned a value.'True'. The value '0' is assigned to the variable 'CandidateId.'The candidate ID begins with '1'.

Self-Verification:

Voters can use the function 'Getcurrentvoter' to verify the status of their registration by supplying their address as an input argument. This function returns all details based on the address that was used to call it. It returns voter address, voter name, whether the voter voted or not, whether the voter is registered or not, and, if the votes were cast, the candidate id for whom the voter voted. The voter can utilise this tool to check on the status of their vote. If the candidate id is different from what they voted for, they can contact the administrator to file a complaint.

Voting:

The most significant function in the project is the vote function.The candidate id for whom the voter wishes to vote will be one of the input elements. The prerequisite for invoking this function is that it can only be accessed by registered voters. That is, the variable registered must be true, whereas the variable 'voted' must be false.

The function sets the 'voted' variable to 'true' and the candidate id variable from '0' to the input candidate id after incrementing the vote count of the candidate whose id is provided as input. Finally, it emits the event 'vote' cast, along with the votes' addresses.

We've also included the 'Time Limit' time variable to give the votes a time limit. The default time is 5 minutes. The time restriction is also a requirement for this function. The maximum time restriction should be less than 5 minutes.

IV. CONCLUSION

In today's environment, stock market forecastingis a highly sought after skill. Many academics have developed a variety of models in order to obtain high accuracy in stock price forecasting. Because the stock market is influenced by a variety of elements, most studies concentrate on a single feature to produce a prediction, but just a few attempt to include many factors. Our suggested system employs deep reinforcement learning and the ensemble approach to forecast stock price increases and decreases based on factors such as historical data, real-time data, and sentiment analysis of linked news. When compared to other machine learning techniques, reinforcement learning produces more efficient, accurate, and better results. The margin of error was tiny in these, making it very ideal for predicting the real stock price.

REFERENCES

[1] K Teja,MB Shravani,Chintarlapallireddy Yaswanth Simha,Manjunath R Kounte "Secured voting through Blockchaintechnology",IEEE Explore,2019

[2] Mohamed Fartitchou; Khalid El Makkaoui;Nabil Kannouf;Zakaria El Allali "Security on Blockchain Technology". IEEE,2020.

[3] Diego Cagigas ,Judith Clifton,Daniel Diaz-Fuentes,and Marcos Fernández- Gutiérrez ."Blockchain for Public Services: A Systematic" 2020 4th International Conference on Electronics, Communication an. IEEE, 2020.

[4] K Teja, MB Shravani, Chintarlapallireddy Yaswanth Simha, Manjunath R Kounte "Secured voting through Blockchain technology".IEEE Explore,2019

[5] Mohamed Fartitchou;Khalid El Makkaoui;Nabil Kannouf; Zakaria El Allali "Security on Blockchain Technology". IEEE, 2020.

[6] K Teja, MB Shravani, Chintarlapallireddy Yaswanth Simha, Manjunath R Kounte "Secured voting through Blockchain technology".IEEE Explore,2019.

[7] Diego Cagigas , Judith Clifton , Daniel Diaz-Fuentes ,and Marcos Fernández- Gutiérrez ."Blockchain for Public Services: A Systematic" 2020 4th International Conference on Electronics, Communication an. IEEE, 2020.

[8] Mohamed Ibrahim,Kajan Ravindran, Hyon Lee,Omair Farooqui,Qusay H, Mahmoud. "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication.." IEEE ,2021.

[9] Ganesh Prabhu S , Nizarahammed.A ,Prabu.S,Raghul.S ,R.R.Thirrunavukkarasu ,P. Jayarajan.. "Smart Online Voting System". IEEE,2021.

[10] Fujioka, A., Okamoto, T., Ohta, K. Heidelberg.