International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 9 ǁ September 2022 ǁ PP. 40-45

Online Voting System Using Blockchain Technology

Ashish ND
PG Student at the National Institute of Engineering, Mysuru, Karnataka, India

Smt Madhu Nagaraj
Assistant Professor, The National Institute of Engineering, Mysuru, Karnataka, India

Abstract-*The outdated paper ballot method and the widely used electronic voting devices can both be replaced by online voting (EVM). In addition to the openness of votes and the privacy of voters, an electronic voting site should provide security and integrity. This study suggests a blockchain-based electronic voting system that overcomes some of the drawbacks of the current voting methods. The report also discusses the current state of certain blockchain voting platforms. The implementation that is currently being used is appropriate for small-scale elections held inside of offices, boardrooms, etc. The implementation makes advantage of Ethereum smart contracts. In this study, smart contracts were developed, tested, and deployed using the truffle framework. For testing, the Ethereum client is Ganache. Here, the browser wallet is Meta-mask.*

Date of Submission: 25-08-2022 Date of acceptance: 09-09-2022

I. INTRODUCTION

This article presents a blockchain-based online voting system that is entirely decentralised and open. A decentralised peer-to-peer network is called blockchain (P2P). The purpose of using blockchain is to do away with centralised control and middlemen. Research is now being done to adapt blockchain to a variety of industries besides finance, including the Internet of Things [1], healthcare, e-voting, logistics, e-commerce, real estate, security, and privacy [2].

A blockchain-based electronic voting system operates on a similar principle as digital wallets. Following identification verification, the system or authority may grant each participant a digital wallet. The wallet that is sent out must have the user credentials and a single coin that represents one vote [3]. The currency in the user's wallet is transferred to the candidate's account or wallet when the user chooses a candidate and casts a vote. The final representation of the votes cast for each candidate is the quantity of coins in his wallet.

Compared to EVM, electronic and internet voting systems can offer more security and integrity [4]. Additionally, it gives users privacy because qualified voters may cast their ballots anonymously using computers or even cellphones. Due to the system being online and entirely transparent, it also increases user confidence. It may also boost the participation of participants.

Blockchain ensures trust by doing away with the requirement for a central server to operate the network and a centralised database. A fully decentralised open ledger system, in other words.

The public ledger, which is permanent and unchangeable, keeps track of all votes cast. It makes sure that once a vote is cast, it cannot be modified. It is almost hard to modify the ledger due of the consensus method since to add a new block, one must first hack all of the prior blocks. Depending on the consensus used, a hacker must infiltrate at least one-third or, in certain cases, even half of the network in order to breach the network [5]. The problems and advantages of several blockchain-based electronic voting system implementations are also covered in this study.

II. MOTIVATION FOR BLOCKCHAIN TECHNOLOGY

Traditionally, a single entity or centralised authority has full control over the database and is responsible for its upkeep. It is capable of altering the database and changing the data. The authority that produced and will be utilising the database is often the same one that maintains it. In such circumstances, the organisation has no incentive to fabricate or manipulate its own statistics. Giving a single authority or institution complete control over a database, however, is not advisable in situations involving money or sensitive information, such as voting.

A central database is simpler for hackers to exploit, even if the company is assured not to make any fraudulent modifications to it. Blockchain makes databases open to the public, allowing anybody to maintain an own copy that can constantly be compared to check for alterations. To preserve consistency, the separate copies must be updated consistently. Blockchain uses a consensus technique to keep a consistent decentralised database.

II. RELATEDWORK

The most advanced blockchain-based electronic voting systems are shown in this section. According to a review of the literature, blockchain-based voting solutions have been put out for use in organisations, communities, and governments.

The Active Citizen initiative for the city of Moscow was introduced in 2014 in Russia [6]. Since then, several surveys have been performed on a variety of topics, including what colour the seats in a new sports stadium should be, among others [7]. A blockchain-based smart contract voting mechanism was implemented in South Korea in 2017 [8]. On a blockchain, all the crucial information, including the votes and outcomes, were kept. No management or centralised authority participated in the process.

Estonia was the first nation to permit the use of an online voting system in 2007. 30% of votes cast in the 2015 legislative elections were cast electronically [9]. Estonian residents' national ID cards are used to verify their identities. These cards have encrypted identification information. With the aid of this technology, Estonian individuals are now able to conduct a wide range of activities online, including e-voting, online banking, and government portal information access. The voters can verify their voting status by inserting their cards into a card reader. The voter can access the voting website on the linked computer after being verified.A voter can visit the website for four days once their login credentials have been verified. The user may vote throughout these four days and may modify their vote many times. After being submitted, the vote goes through a forwarding server and is then encryptedly stored on a server. These votes are sent to a counting server that is disconnected from the network once the online voting session has ended. The votes will be tallied on this server, and the results will be shown. This electronic voting mechanism, however, may provide certain hazards. On client side computers, there may be malware that keeps track of and tampers with the cast votes. The Estonian government also intends to employ blockchain for other purposes, including the upkeep of electronic health data and online patient monitoring systems.

A voting system built on the blockchain was created in 2018 by Agora, a Swiss blockchain firm. It received some testing during the 2018 general elections in Sierra Leone [10]. A comprehensive, end-to-end verified blockchain is Agora. It is made to give corporations, governments, and organisations access to an online voting system. With this blockchain-based electronic voting system, qualified voters can buy tokens from organisations or the government.

There are other firms, such the Abu Dhabi Stock Exchange, FollowMyVote, TIVI, Blockchain Voting Machine [11], etc., working on additional initiatives to build blockchain-based electronic voting systems.

The Boardroom Voting with Maximum Voter Privacy was a proposal made by McCorry et al. in 2017 [12]. It offers a self-tallying voting process using smart contracts. The decentralised Open Vote Network (OVN), which runs on the blockchain, is constructed using Ethereum.

A decentralised blockchain-based voting system called Netvote [13] was suggested by Jonathan et al. in 2018. Decentralized applications (dapps) are used as the user interface, and it is built on the Ethereum network. The writers recommend three dapps. One is the admin dapp, used by management to establish policies, regulations, and other things. Voter is another dapp that allows people to register and cast ballots on their own. The Tally dapp is then used to tally and announce the results of the election. But the foundation of this system is a private blockchain.

III. IMPLEMENTATION DETAILS OF BLOCKCHAIN BASED E-VOTING

The design considerations for establishing a blockchain-based electronic voting system are covered in this section. A brief introduction to Ethereum and smart contract technologies follows.

A. Designconsiderations

The following considerations should be made while developing an electronic voting system:

- The electronic voting system need to validate only legitimate voters and confirm their identities.
- Ineligible candidates shouldn't be able to use the electronic voting system.
- The technology should prohibit multiple voting by allowing each voter just one opportunity to cast a ballot.
- Voters should have total privacy, and votes shouldn't be able to be tracked.
- It shouldn't let anybody to interfere with the votes they cast.
- The system should not permit the control of counting by a single authority.

B. Ethereum

Blockchains may be divided into two groups: permissioned blockchains and permission-less blockchains. Private blockchain networks with participation limits are known as permission-ed blockchains. Public blockchains are those that don't require permission. There are no limits on who may view or write on the

blockchain ledger database in public blockchains. A public, decentralised blockchain network called Ethereum exists.

Ethereum is a platform that, in essence, enables developers to create decentralised apps utilising blockchain technology. It is a blockchain network without permissions. The many Ethereum account types are discussed in this section. There are two different kinds of accounts on Ethereum:

- ExternalAccounts
- ContractAccounts

A user-controlled account is one that is externally owned. It stands in for a network's external agent, such as users, miners, etc. RSA-style public-private key encryption is used to control these accounts. Users interact with the Ethereum blockchain mostly through external accounts.

A smart contract, which is a body of code that governs blockchain, is a contract account. These are regarded as accounts since they are kept at a certain location. Either certain external accounts or other contract accounts will always invoke a contract account. These contracts were created using solidity and serpent, two high level scripting languages.

These two accounts can both hold ether. Ethereum's native cryptocurrency, Ether, is represented by the symbol "ETH" on exchanges. In the Ethereum network, it is employed for services and transaction fees. These are used to complete transactions or pay for gas. A payment method for computational labour completed for the execution of a smart contract or for some transactions is gas, an intermediate token. Ether may be used to buy gas.

C. SmartContracts

Self-executing software, or smart contracts, is created inside of blockchains. These are used for code of conduct agreements between two parties and are comparable to customary commercial contracts. When the predetermined criteria are satisfied, the smart contracts immediately go into action. Without the need for a centralised authority, smart contracts enable the trustworthy execution of agreements and transactions between unreliable or unknown parties.

Solidity language is used for writing smart contracts. It is an object-oriented language with syntax that is comparable to Python or JavaScript. Compared to traditional contracts, smart contracts provide a number of advantages, including cost savings and increased productivity. Smart contracts are well-liked because they promote confidence between parties and are simple for all users to verify.

D. WorkingofBlockchainVotingSystem

RVoter and candidate registration must be completed in advance. Before creating accounts, identity verification should be performed. A currency or token should be presented to authenticate eligible users after identification has been confirmed [14]. Each user may only cast a single vote using this coin or token. The verification procedure on the blockchain will make sure that it is impossible to spend this token twice. Therefore, a user cannot vote more than once. The blockchain-based electronic voting system is decentralised. The elections are not managed by a central body.

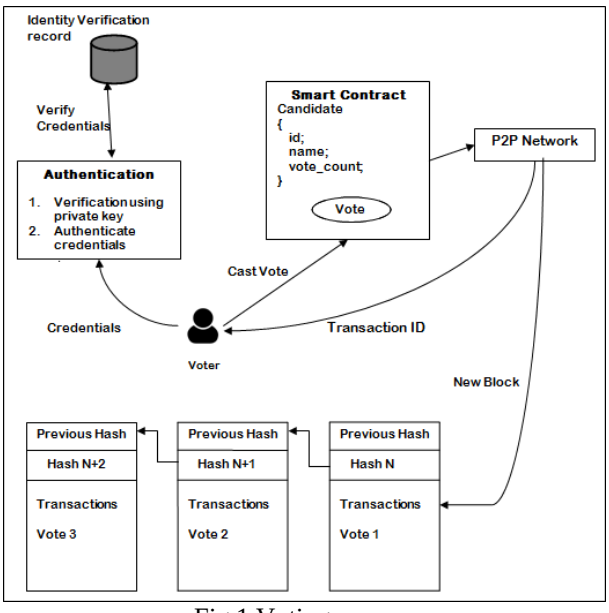

Fig.1.Votingprocess

E. Implementationin Ethereum

On the Ethereum blockchain, a decentralised application called the e-voting dApp was created. Solidity-basedsmart contracts for Ethereum are used to cast ballots. Voting is done using a client-side user interface that uses Ethereum accounts. This approach tests the smart contracts before deploying them on the blockchain using the truffle framework network environment for blockchain. Building smart contracts, compiling built-in contracts, linking those contracts, and deploying them can all be done using the truffle development framework.

Truffle ecosystem includes ganache. For the development of Ethereum, it offers a private blockchain. It might be considered an Ethereum client. The decentralised application developed on truffle may be tested using it. While creating decentralised apps, it may be utilised to distribute contracts. It also makes it easier to test blockchain and smart contract functionality. An Ethereum client like Geth may be used to deploy the application after it has been tested on Ganache. A local and virtual blockchain are available for testing with Ganache. There are 10 external user accounts available. A distinct Ethereum address and corresponding private key are given to each account in Ganache. Each account has 100 "fake" ethers already loaded.

CLI and UI are the two versions of Ganache. For convenience, UI version was chosen in this implementation. An Ethereum node may be operated similarly to ganache. It resembles a computer node. Wallets and Ganache can be linked for transactions. This implementation makes advantage of Meta-mask. A Chrome addon called Meta-mask can connect to Ethereum nodes and access user wallets. RPC is how Meta-mask communicates with Ethereum nodes.

After a smart contract is activated, the blockchain is updated via migrations. We must construct a migration, which is a numbered Java script file, for each smart contract. These files are automatically called in order by the truffle framework. The migration file links the following to the smart contract:

```
var TempContract = artifacts.require("./TempContract.sol");module.exports = function(installer)
{installer.deploy(TempContract);
};
```

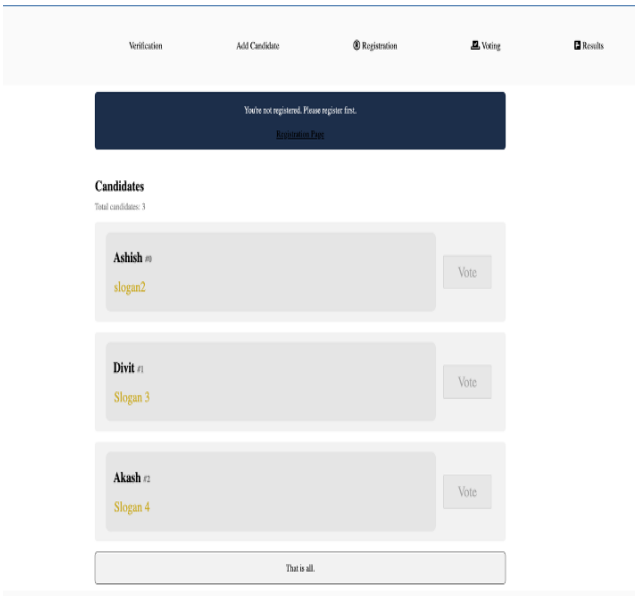

Fig.2.Screenshotofthevotingportalscreen

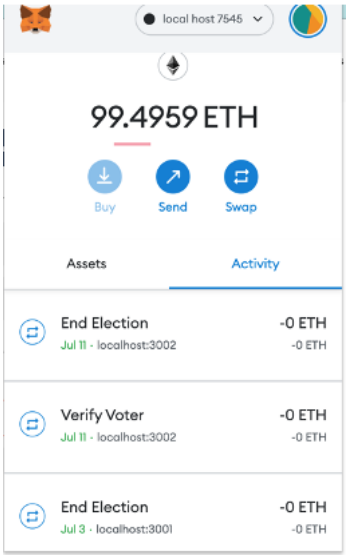

Fig. 3.Screenshotofthemetamaskconfirmationnotificationwhenavotercasts vote

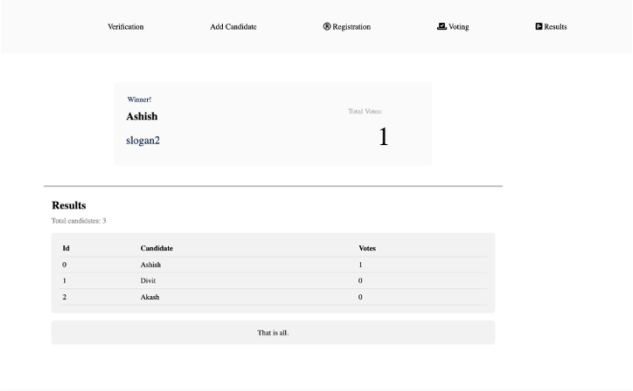

Fig.4.Screenshotoftheelectionresultafterusercastsvotesandconfirmsthevote

IV. BENEFITSANDCHALLENGES

The advantages of a blockchain-based electronic voting system include:

- Votes that have been kept are tamper- and immutable-proof.
- It protects the anonymity and privacy of the voter.
- The use of electronic voting systems may increase voter engagement.
- It could increase effectiveness and provide quicker outcomes.
- It encourages the system's openness and clarity..
- It removes uncertainties brought by by incorrect or confusing voting selections made on paper ballots.
- the complexity of blockchain technologies may limit their universal support
- Public auditing of voting results is available.

However, the complexity of blockchain technologies may limit their widespread acceptance. Another issue with e-voting systems is continual broadband availability. The abilities of the digital user may also be a problem. for big Blockchain uses a lot of energy for authentication and validation of users. Therefore, additional study is needed on the consensus of implementing a blockchain-based voting system for national electronic voting.

V. CONCLUSIONANDFUTUREWORK

This paper introduces an Ethereum-based blockchain-based electronic voting system. It demonstrates how centralised voting system constraints may be addressed by blockchain technology. In this solution, voter accounts, candidate information, and votes are stored using an Ethereum blockchain network and database. In this implementation, smart contracts are used. On a virtual client, this implementation has been tried. Future testing on the Ethereum test network with a large number of accounts is possible. Future research should evaluate the viability of a blockchain-based electronic voting system for a significant election.

REFERENCES

[1]. Francesco Restuccia, Salvatore D'Oro, Salil S. Kanhere, TommasoMelodia, and Sajal K. Das, "Blockchain for the Internet of Things:Present and Future," IEEE Internet of Things Journal, vol. 1, no. 1,pp.1-8,January2018.

[2]. YiyunZhou, Meng Han, Liyuan Liu, and Wang Yan, "ImprovingIoT Services in Smart-Home Using Blockchain Smart Contract," inIEEEConfs.onInternetofThings,GreenComputingandCommunications,Cyber,PhysicalandSocialComputing,SmartData, Blockchain, Computer and Information Technology, Congresson Cybermatics,pp.81-87,2018.

[3]. NirKshetriandJeffreyVoas,"Blockchain-EnabledE-Voting,"IEEE Software, pp.95-99,2018.

[4]. FriorikP.Hjalmarsson, Gunnlaugur K.Hreioarsson,MohammadHamdaqa,andGisliHjalmtysson,"Blockchain-BasedE-VotingSystem,"inIEEE11thInternationalConferenceonCloudComputing,pp.983-986,2018.

[5]. BayuAdhiTama,BrunoJoachimKweka,YounghoPark,andKyung-HyuneRhee,"ACriticalReviewofBlockchainandItsCurrentApplications,"inIEEEInternationalConferenceonElectrical Engineering and Computer Science (ICECOS) 2017, pp.109-113,2017.

[6]. M.Hochstein,"Moscow'sBlockchainVotingPlatformAddsServiceforHigh-RiseNeighbors,"CoinDesk,15Mar.2018;https://www.coindesk.com/moscows-blockchain-voting-platform-adds-service-for-high-rise-neighbors,2018.

[7]. M.D.Castillo,"RussiaIsLeadingthePushforBlockchainDemocracy," CoinDesk, 2018; https://www .coindesk.com/russias-capital-leading-charge-blockchain–democracy, 2018.

[8]. "SouthKoreaUsesBlockchainTechnologyforElections,"KryptoMoney, https://kryptomoney.com/south-korea-uses-blockchain-technology-for-elections,2017.

[9]. AndrewBarnes,ChristopherBrakeandThomasPerry,"DigitalVotingwiththeuseofBlockchainTechnology",https://www.economist.com /sites/default/files/plymouth.pdf,2016.

[10]. Agora: Bringing our voting systems into the 21st century Availableat:https://agora.vote/Agora_Whitepaper_v0.1.pdf,2017.

[11]. Hiren M Patel, Milin M Patel, Tejas Bhatt, "Election Voting UsingBlockChainTechnology",InternationalJournalofScientificResearch andReview, Volume07, Issue05,pp1-4,May2019.

[12]. Patrick McCorry, Siamak F. Shahandashti and Feng Hao,"A SmartContractforBoardroomVotingwithMaximumVoterPrivacy",Published in: Financial Cryptography and Data Security, Springer,2017.

[13]. JonathanAlexander,StevenLandersandBenHowerton,"Netvote:ADecentralizedVotingNetwork",https://netvote.io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf,2018.

[14]. D. Khader, B. Smyth, P. Y. Ryan, and F. Hao, "A fair and robustvoting systemby broadcast", in5thInternational Conference onElectronic Voting,Vol. 205,pp285-299,2012.