JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 05, 2021

BLOCKCHAIN USING A PUBLIC BLOCKCHAIN TO PROVIDE PRIVACY AND TRANSPARENCY IN E-VOTING

Mrs.T.Sarika,Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,
E-Mail-id sarika.tuniki@cmrec.ac.in

Yogesh Singh Rajpurohit ,188R1A1260
S.Nithin Reddy ,188R1A1252
G.Akshay Kumar,188R1A1216
CH.Sai Kumar, 188R1A1209

Abstract

Since then, there have been some ways of voting. Over the world, paper ballots are the most common voting format. Only in the past ten years have electronic voting methods gained popularity, and they remain unaddressed. E-voting systems have issues mostly with functionality, security, legitimacy, and openness. Estonia is the innovator in this area and might be regarded as the cutting edge. Nevertheless, there aren't many alternatives that use blockchain. All of the aforementioned issues can be solved with blockchain, which also offers benefits like immutability and decentralisation. The primary issues with blockchain-based technology used for electronic voting are their narrow focus or a lack of testing and comparison. In this paper, we introduce a general-purpose e-voting platform built on a blockchain. Blockchain uses it to the fullest extent possible and has the capacity to manage all procedures. When the voting process has begun, the platform operates as though it is completely autonomous and decentralised, with no potential for interference. Although the data are completely visible, homomorphic encryption protects the voters' identities. We put our approach to the test on three distinct blockchains and compared the results. The findings demonstrate that both public and private blockchains may be used with only a little speed difference. The main innovation of our solution is the fully decentralised management of the e-voting platform through blockchain, transparency of the entire process, and privacy and security of the voters thanks to homomorphic encryption.

Key words : Ethereum, smart contracts, blockchain, elections, homomorphic encryption, and Hyperledger Composer.

I. INTRODUCTION

The development of e-voting technologies is still in its infancy. We picked this topic not just because it is new, but also because there aren't many solutions available to issues with e-voting. These days, e-Government development is gaining popularity. Nevertheless, if essential services for residents like elections do not go electronic, such a system is not practical. One of the major public areas that blockchain technology has the potential to alter is e-voting [1]. E-voting also brings with it new problems that need to be solved. With electronic voting come new problems that must be solved. One of them is election security, which must be at least as secure as the traditional voting methods using ballots.

Because of this, we have chosen to have secure elections where voters won't have to worry about fraud or other electoral irregularities.

Blockchain is frequently cited as an example of safe technology being employed in an online context in recent years. All election procedures are managed by our voting system using blockchain.Its key benefit is that no trust in the centralised entity that established the elections is required. The outcome of the election under our system cannot be impacted by this authority. The outcome of the election under our system cannot be impacted by this authority. Another difficulty with electronic voting is the lack of system transparency, which undermines voter trust [2].Blockchain offers a completely transparent solution to this issue, enabling everyone to view the methods used to store data and manage it. This technology is more suited than the traditional e-voting platform without blockchain from a security perspective.

The following is the breakdown of the article. A quick overview of the current blockchain electronic voting options is shown in Section II. We outline the design of our solution and all of its components in Section Ill. Part IV contains the evaluation, and Section V has a discussion of the findings and further conclusions.

II. EXISTING SYSTEM

Blockchain is a distributed ledger of data that is often used. The immutability of the records that have already been recorded in blocks is the fundamental tenet of the blockchain. Data integrity is provided via the chaining of blocks, which is ensured by advanced encryption. The kind of network connectivity is another characteristic. Client-client communication is the mechanism used by network nodes. There is no need for confidence in this individual because there is no intermediary facilitating communication between clients. The real identity of the network participant is unknown [3]. This section will examine some of the current blockchain-based voting system options that are currently available.

a. NETVOTE

Internet voting systems, often known as "Netvote" systems, are created to let voters cast their ballots online rather than visiting to a physical polling place. In the Ethereum network, Netvote is a decentralised application for voting that is built on blockchain technology [7]. Users of the network can access a decentralised application environment through Netvote. Create elections, establish election regulations, establish voter registration requirements, build ballot boxes, and set up voting with a DApp made for administrators. Voters may register for elections and cast their votes for the preferred candidate using a DApp. You can use the relevant programme to examine the results when the elections are over. The programme gives the administrator a choice between three different voting methods. Open elections are the first type, and everyone with an account on the Ethereum network is eligible to participate. Private elections, in which only registered voters may cast ballots, are the second type. Only voters who possess the necessary number of valid tokens issued just for the elections are permitted under the final option. Each election in Netvote is made up of many Ethereum network-deployed smart contracts. An administrator creates these smart contracts using his DApp. The Vote Gateway, a technology offered by Netvote, is used to confirm voters' identities. The voter uses his DApp to transmit his/her signed ballot. The Vote Gateway chooses the voter's private key from the vault where this particular private key is kept if the voter is registered. Netvote is a good solution for both state elections and institutions. The open blockchain of Ethereum is used by Netvote. Refactoring Netvote's architecture is necessary. It could be interesting to use private blockchain elections when the rate of transaction processing rises dramatically.

b. OV-net

The online voting platform OV-net has been utilised in a number of nations, including Norway and Estonia. A 2-round decentralised election mechanism called OV-net (Open voting network) [9] is developed on the Ethereum blockchain. This procedure offers a number of benefits. One of them is the protocol's independent vote-counting without the required authorization. Privateness is enhanced. Only in the unlikely event that every other node in the network is fake might a voter's decision be made public. Users can check each other's adherence to the protocol. The procedure is divided into five sections:

1. Setup - The election's administrator is in charge of starting the smart contract with a legitimate voter list.
2. Registering - Voters will email their electoral key and validate it using zero-knowledge proof (ZKP).Ethereum keeps the electoral key and validates the ZKP's accuracy.
3. Voting: Each vote is transmitted in an encrypted form. This vote can be a 1 (yes) or a 0 (no) (no). Ethereum checks sure the vote is limited to the choices of 1 or 0, after which it records it.
4. Voting Count: When every vote has been cast, Ethereum tallies the results.

A well-managed protocol called OV-net enables several essential e-voting tasks. It does, however, have a number of drawbacks. There are just two possible votes: yes or no. A significant portion of voters are also unable to vote in OV-net due to the way it was implemented. The requirement to cast a ballot for every voter is another drawback. The elections could not be judged or counted if one voter did not cast their ballot. In recent years, a number of e-voting methods have been developed, although the majority lack documentation and details on how the service functions inside. Follow my Vote is one of the services. This method does not provide comprehensive answers as to how it operates on a blockchain network. BitCongress is another service that was created to function with a variety of protocols, including Bitcoin and Mastercoin. Eventually, neither of the apps was implemented. The only successful project that was partially demonstrated in the state elections was created by the Swiss company Agora.

III. PROPOSED SYSTEM

The suggested blockchain voting system takes into account all voting needs and is made to work for any election, including those for president, student parliament, etc. Elections can take place in multiple rounds, and ideally a public blockchain is used. Several forms of blockchain can take the place of the public blockchain, but the recorded data (votes) must still be simple for any user to verify.

Each observer with an interest in the blockchain voting is represented by the user. Three crucial roles-vote publisher, key authority, and voter are identified in our proposed system. Any of these three positions may stand in for a user, a business, or an organisation. Because they can both be the same company or person, the duties of vote publisher and key authority can be combined into one job. According to a vote arrangement, the voter goes to the polls. Vote publishers, which are a part of the smart contract, are responsible for configuring the votes. Before to publishing the smart contract, the vote publisher must possess all cypher keys. A good working relationship is necessary between the key authority and the vote publisher. Voter and vote publisher get all cypher keys created and distributed by the key authority. As of now, the distribution channel route must now be protected and should not be open to outside interference.

Figure 1 depicts the high-level voting system architecture. Roles, elements, and linkages between them are all depicted. The architecture includes the following elements: eID , results interface, key authority API, and blockchain (all necessary) (optional). A smart contract, which is a component of the blockchain and is in charge of processing and evaluating votes, is a specialised component.

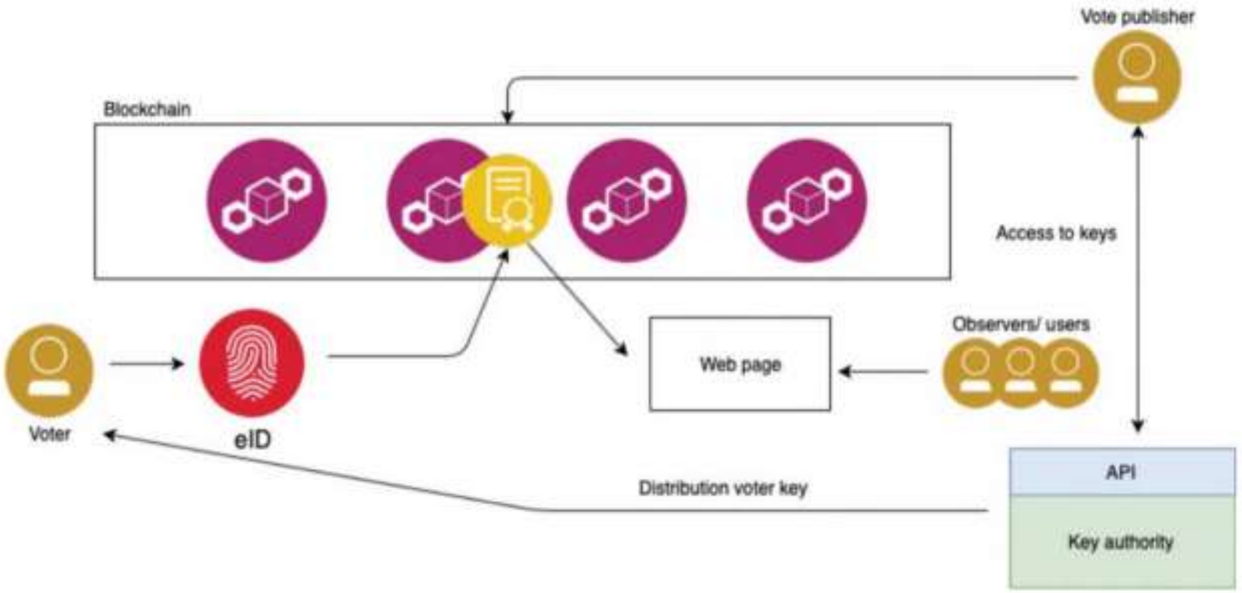


Fig 1:Architecture

An optional module that may be included in the key authority organisation is the key authority API. This API helps voters and vote publishers get a key to access the votes as well as a public key for homomorphic encryption. These keys may be given out manually or in another manner. The component is merely optional and not necessary in the architecture because of this.

1. Blockchain

The blockchain component executes voting processes and represents the whole architecture for storing data. A public blockchain like Ethereum or a private blockchain like Hyperledger can be used to build a blockchain. The benefit of the public blockchain is that it gives all users access to information about transactions and blocks, which gives it more credibility than the private blockchain. This assurance is made in the perspective of a common user who wants to view all the information and is not technologically sophisticated. The private blockchain can offer the same level of assurance, but a company must demonstrate it with data. The use of blockchain is not constrained by the suggested design. The same degree of confidence may be offered by both kinds of blockchain. The entity responsible for organising elections chooses the platform.

2. elD

This element gives users access to the blockchain so they may conduct voting. We take into account eID in the architecture, which serves as a gateway to the blockchain network. Public and private keys are provided to the user by the key authority and are contained on the ID card. The typical public address of a wallet on the blockchain is represented by the public key. Only the voter is aware of the secret key.

3. Results interface

An interface to the results is represented by this component. The interface has to have access to the blockchain and provide users and observers with information. Vote results are included in the data, and users should be able to view transactions on the blockchain as it should be transparent about all transactions. Just the final findings are displayed, and the results are presented graphically for easier interpretation. As a result of the homomorphic encryption being used, live results are not available.

IV. IMPLEMENTATION

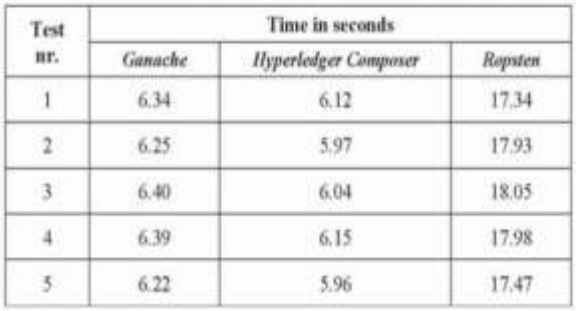
We have chosen to put the intended service into practise following the design phase. We have developed two test cases to ensure that our application is functional. The major objective was to evaluate the solution's general functioning, security, and speed. Our testing setup included a MacBook Pro running macOS Mojave (10.14.3), the Chrome web browser with JavaScript enabled, and the MetaMask plugin installed. A straightforward interface for interacting with the Ethereum network is provided by MetaMask. We have built a small Ethereum network using Ganache for testing reasons. We released the smart contract to the Ropsten test network once all automated truffle testing were successful.

Basic unit tests, which tested the smart contract and its behaviour for errors, are covered in the first test case. 1000 fake test users were used to implement it, and they cast their votes normally, just like actual people would. In addition, test cases for duplicate voting, voting without authorization, looking at the results after the election, and second-round voting for candidates who advanced from the first round if it was unsuccessful, that is, if none of the candidates received 50% or more, were all conducted.

The second test case was timing how long it would take a real individual to cast a ballot. The process included launching the voting online application, selecting a candidate, casting your ballot, uploading your vote to the blockchain, and registering your vote. The test was carried out by integrating smart contracts into three distinct blockchains: Ropsten, a live Ethereum test network, Hyperledger Composer, and Ganache, a local Ethereum network.

A running script for automated voting of 15 people per second was present in the background.We tried to recreate genuine scenarios that may occur in actual elections when we ran our script. The test scenario was run five times for each blockchain, and Table I shows the test results. It should be noted that the Ropsten network's average block duration, which is about 12 seconds, has an impact on the difference in timings.

TABLE I. COMPARISON OF VOTING TIME IN DIFFERENT BLOCKCHAINS



Test nr.	Time in seconds		
	Ganache	*Hyperledger Composer*	*Ropsten*
1	6.34	6.12	17.34
2	6.25	5.97	17.93
3	6.40	6.04	18.05
4	6.39	6.15	17.98
5	6.22	5.96	17.47

V. CONCLUSION

Although there are very little variations in network latency, they are so small that public blockchain offers greater advantages in this type of voting system since the data is accessible and anybody can view it in real time. A private blockchain is a little bit faster, but because it only operates where the authority wants it to, it partially centralises and undermines the trustworthiness of the entire system. The data reveals that the median timings to add a single voice are 6.34 seconds for Ganache, 6.05 seconds for Hyperledger Composer, and 17.75 seconds for Ethereum Ropsten (median 17.93 s). Both the block time and the consensus algorithm in use have an impact on these periods.

VI. REFERENCES

[1] M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda, “Voting Processwith Blockchain Technology: Auditable Blockchain Voting System,” inLecture Notes on Data Engineering and Communications Technologies,pp. 233-244, Springer, Cham, 2019.

[2]] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram and Konstantinos Markantonakis “E-voting with Blockchain: An e-voting protocol with decentralization and voter privacy” 2018.

[3] N. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,”IEEE Software,vol. 35, pp. 95-99, jul 2018.

[4] R. Perper, “ Sierra Leone is the first country to use blockchain duringan election - Business Insider,” 2018.

[5] S. Landers, “Netvote: A Decentralized Voting Platform - Netvote ProjectMedium,” 2018.

[6] B. Singhal, G. Dhameja, and P. S. Panda, “How Blockchain Works,” inBeginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[7] P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract forBoardroom Voting with Maximum Voter Privacy,” inLecture Notes inComputer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[8] Z. Brakerski and V. Vaikuntanathan , “Efficient Fully Homomorphic Encryption from (Standard) LWE” ,SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.

[9] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,”Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[10] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” tech.rep., 2008.