International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Blockchain Based E-Voting System

Prof. Mrunal Pathak[1], Amol Suradkar[2], Ajinkya Kadam[2], Akansha Ghodeswar[2], Prashant Parde[2]

[1]Assistant Professor at Information Technology Department, AISSMS Institute of Information technology, Pune, Maharashtra, India

[2]B.E. Scholar, Information Technology Department, AISSMS Institute of Information technology, Pune, Maharashtra, India

Article Info
Volume 8, Issue 4
Page Number : 246-251

Publication Issue
July-August-2021

Article History
Accepted : 08 July 2021
Published : 14 July 2021

ABSTRACT

Developing a dependable voting system which offer neutrality and privacy of content and anonymity and effective results has been challenge over the time. e-voting is one of the latest version techniques for implementing tamper proof system with for secure voting. blockchain can be considered as a backbone for developing secure voting system, because blockchain technology is a decentralized system an entire system is owned by many users. blockchain based voting system, there will be no single point of failure or point of manipulation. In this paper we are going to study the our proposed system that uses state of art blockchain Framework for voting. the proposed solution for voting based on blockchain is suitable for small scale elections. implementation is a comprehensive collection of Technologies like truffle framework for development, testing and deployment, Ganache is used etherum side for providing etherum testing accounts and metamask browser extension for browser synchronization and as a browser wallet.

Keywords : Blockchain, ethereum, smart contracts, e-voting, solidity

I. INTRODUCTION

Voting is a base of democracy in any country. voting is indispensable element of democracy. so voting must be conducted in a free and fair fashion. for the voting process says must be effective enough that it cannot be tempered. current election method has ballot boxes to store votes. This process is offline and centralised. there is a single source of storage. the proposed system on blockchain which overcome the most drawbacks existing systemblockchain based e voting system has Same Idea as a digital wallet . the officials assign an digital wallet to each participants after verifying their identity. the wallet access by private key provided to voter. every voter has some coins in their wallet. voting process will require coins which will be spend on cast vote method e-votiong system offers increased integrity and security than EVM. it also provides an anonymity to voters. it also provide and feature of voting from an remote placeas we are using blockchain based system and blockchain is a decentralized distributed ledger so it is completely

eliminate the need of centralised storage and centralised database thus ensures trust.

II. II.Related work

This section contains some state of the art relevant e-voting systems that use blockchain as a service.In 2014, Active Citizen program was launched in Russia, the city of Moscow's . In 2017, a smart contract based blockchain enabled voting system was used in South Korea . All the important data was stored on a blockchain like votes and results. There wasn't any involvement of management or central authorityin the process.

In 2018 , Agora is anvoting solution designed for governments and institutions which is based on end-to-end verifiable blockchain.On the blockchainAgora uses their own Token for elections,where governments and institutions purchase these tokens for each individual eligible voter.

Online voting system is developed in EstoniaIn 2007 and Estonia became the first country to allow use ofonline voting system.In 2015 parliamentary elections 30% of votes were casted through e-voting system.In Estonia they wereusing the national ID card of citizens for identity verification.The information in the identity cards was in encrypted manner. Due to this system Estonian citizens was ableto perform many tasks online such as online banking services,e-votingand access information on government portals.For verification the citizens can enter their card into a card reader in voting system. After verification the voter gets access to the voting website on the connected computer. A voter has access to the site for four daysAfter verifying user credentials.

User can cast its vote and can even change it several timesin these four days. After submitting the vote, it passes throughforwarding server and stored in a server in encrypted form.These votes are transferred to a counting server which is disconnected from.

III. IMPLEMENTATION DETAILS OF BLOCKCHAIN BASED EVOTING SYSTEM

A. Design considerations

Following points are important and should be considered while implementing e-voting system:

1)The e-voting system should verify the identity of voters and authenticate only eligible voters.
2)The e-voting system should not allow access to invalid candidates.
3)Any voter should get only a single chance to vote i.e. system should prevent double voting.
4)It should provide complete privacy to voters and the votes should not be traceable.
5)It should not allow tampering with the votes casted by anyone.
The system should not allow single authority control on counting.

B. Ethereum

Blockchains can be classified into two categories: permission-ed and permission-less. Permission-ed blockchains are private blockchain network with restrictions on participation. Permission-less blockchains are public in nature. In public blockchains there are no restrictions such that anyone can read or write on blockchain ledger database. Ethereum is a public decentralized blockchain network. Basically, Ethereum is platform that allows programmers to build decentralized applications using blockchain technology. It is a permission-less blockchain network. This section describes the types of accounts used in Ethereum. Ethereum has two account types: x External Accounts x Contract Accounts An externally owned account is a user controlled account. It represents an external agent of

network like users, miners etc. These accounts are regulated with a public-private key cryptography like RSA algorithms. Mainly external accounts are used by users as a means to interact with the Ethereum blockchain. A contract account is a smart contract which is a collection of code that regulates blockchain. These are stored at a specific address, hence considered as accounts. Contract accounts are always either invoked by some external accounts or by other contract accounts. These contracts are written in high level scripting languages such as Solidity and Serpent. Both of these accounts can store Ether. Ether is the crypto currency of Ethereum, denoted by "ETH" in crypto currency exchanges. It is used for transactions fee and services in the Ethereum network. These are used to pay Gas or transactions done. Gas is an intermediary token used to make payment for computational work done for executing a smart contract or for some transactions. Gas can be purchased using Ether.

C. Smart Contracts

Smart contracts are self executable code written inside blockchains. These are similar to conventional business contracts that are used for code of conduct agreement between two parties. The smart contracts execute automatically when the defined conditions are met. Smart contracts help to carry out agreements and transactions in a trusted manner among the untrusted or unknown parties without the requirement of central authority. Smart contracts are written using Solidity language. It is an object-oriented language, and its syntax are similar to JavaScript or Python. Smart contracts have several benefits over conventional contracts like cost saving, and improved efficiency. Smart contracts are popular as they are easily verifiable by all users and ensure trust among parties.

D. Working of Blockchain Voting System

Registration process of voters and candidates is to be done in advance. Identity verification should be done before creating accounts. After identity verification, authorized person should authenticate eligible users by proving a coin or token Using this coin or token each user can vote only once. Blockchain's verification process will ensure that double spending of this token is not possible. So any user cannot vote multiple times. The e-voting system based on blockchain is decentralized. There is no central authority to conduct the elections.

E. Implementation in Ethereum

The e-voting decentralized application, or dApp, is built on the Ethereum blockchain. Ethereum smart contract is written in Solidity for casting votes. A client-side user interface is built to use Ethereum accounts to cast votes. Truffle Framework is used in this implementation to test the smart contracts and deploy them to the blockchain. Truffle framework facilitates to develop, test and deploy decentralized applications. It provides a development environment for blockchain network. Truffle development framework can be used to build smart contracts, compile built-in contracts; link and deploy those contracts. Ganache is part of Truffle ecosystem. It provides a private blockchain for Ethereum development. It can be seen as an Ethereum client. It can be used to test the decentralized application built on truffle. It can be used to deploy contracts while developing decentralized applications. It also facilitates to run tests on blockchain and smart contracts.

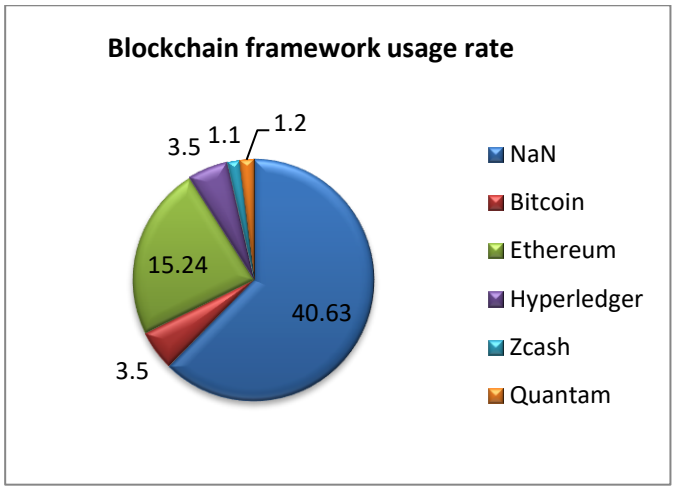
Once the application is tested on ganache, it can be deployed on Ethereum client like Geth. Ganache provides a local and virtual blockchain for testing. It provides ten external user accounts. Each account in Ganache has been assigned a unique Ethereum address and a private key associated with it. All the accounts come preloaded with 100 'fake' ethers.

Ganache comes in two versions, CLI and UI. This implementation has used UI version for simplicity. Running ganache is similar to running an Ethereum node. It is like a virtual node. Ganache can be connected with wallets for transactions. For this implementation, Meta-mask is used. Meta-mask is a chrome extension, which connects to Ethereum nodes and reads user wallets. Meta-mask uses RPC to connect with Ethereum nodes. Migrations are used to update the blockchain whenever a smart contract is deployed. For each smart contract we need to create a migration which is a numbered java script file. Truffle framework automatically calls these files sequentially. The smart contract is associated in the migration file as following : var TempContract = artifacts.require ("./TempContract.sol"); module.exports = function (installer) { installer.deploy (TempContract) ; }; number of users' authentication and validation, blockchain requires much energy. So using blockchain based voting system for national e-voting require more research on its consensus.

IV. Analysis

Blockchain systems enable the event of blockchain-based applications. Bitcoin, Ethereum, Hyperledger and R3 Corda square measure the foremost famous blockchain frameworks. We tend to try to seek out that systems measure largely most well-liked for analyzing the main points of the chosen papers. However, we tend to find that almost all the papers containing general definitions, and there have been less data on the technical implementation details [2]. Several studies tackle the plan of blockchain primarily based e-voting and general problems related to with it. There looks to be a general accord on the concept that blockchain may be applied in e-voting systems. However, technical details and implementation proposals aren't expressly expressed. with all, supported the studies the blockchain platform usage distribution may be seen in Figure.

V. METHODS AND MATERIAL



Gas Cost and Time Analysis

Yuxian Zhang has performed gas value, and time analysis of his system they selected to deploy and check the consent the Ethereum non-public chain. The consumption of Gas and cash for a 40-person election [1]. They calculate the period worth needed for the dealing supported the Gas worth provided by ETH filling station and also the current ETH worth. Gas worth = seven gwei, 1ETH=607.76USD, A and V represent the operations of the administrator and also the elector severally. The results show that it takes concerning $20.49 to carry such an election, and also the administrator must pay concerning $3.41[1]. Meanwhile result's shown in Figure. Since their system don't use advanced calculations and zero-knowledge proofs in contracts, the number of Gas needed to execute contracts is greatly reduced, and this value is appropriate to the organizers, and participants of the election[1].

Operation	**gas Cost**	**gas Cost**
Deploy(A)	3,328,566	6,088,493
Initialize(A)	2,705,384	22,993,368
Send Blind Message(v)	54,780	3,773,528
Send Signature(A)	1,821,960	68,149,05

Send Unblind Signature(V)	42,778	1,770,372
Send Final Whitelist(A)	1,770,372	3,773,528
Register(V)	74,352	553910
Begin Vote(A)	28 849	36796
Vote(V)	553910	146,872
Begin Tally(A)	28,476	553,910
Tally(A)	553,910	654932
Administrator Total	10,237,517	40,915,932
Voter Total	274,693	6,244,679
Election Total	21,225,237	47160611

VI. BENEFITS AND CHALLENGES

Blockchain based e-voting system provides following benefits:

1)Votes are cryptographically secured.
2)Votes once stored are immutable and tamper-proof.
3)It preserves voter's privacy and anonymity.
4)E-voting system may improve active voter participation.
5)It may improve the efficiency and allow faster results.
6)It promotes transparency and clarity to the system.
7)It eliminates ambiguities arising from wrong/unclear choices made on paper ballots.
8)Voting results are publically auditable.

However, blockchain systems are complex in nature which may hinder its wide acceptability. For e-voting systems continuous broadband access is another concern. Another issue can be the digital user skills. For large number of users' authentication and validation, blockchain requires much energy. So using blockchain based voting system for national e-voting require more research on its consensus.

VII. CONCLUSION AND FUTURE WORK

This paper presents a blockchain based e-voting system that runs on Ethereum. It shows that blockchain technology can overcome limitations of centralized voting systems. This implementation uses Ethereum blockchain as a network as well as database for storing voter's accounts, candidate details and votes. This implementation makes use of smart contracts. This implementation is tested on virtual client. In future it can be tested on Ethereum test net with large number of accounts. In future work, the feasibility of blockchain based e-voting system for large-scale election should be analyzed.

VIII. REFERENCES

[1]. F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[2]. C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.

[3]. K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777471.

[4]. R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and

Applications (TSSA), Lombok, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.

[5]. 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. https://doi.org/10.1007/978-3-030-29035-1_54

[6]. 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, 1–1. doi:10.1109/tdsc.2020.2979856

[7]. 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, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[8]. Y. Zhang, Y. Li, L. Fang, P. Chen and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1252-1257, doi: 10.1109/ICCC47050.2019.9064387.

[9]. T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75, doi: 10.1109/ICIMIA48430.2020.9074942.

[10]. Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.

Cite this article as :

Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde, "Blockchain Based E-Voting System", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 4, pp. 246-251, July-August 2021.

Journal URL : https://ijsrst.com/IJSRST2183200