International Journal of Innovation Engineering and Science Research
(ISSN: 2581-4591)
www.ijiesr.com

Decentralised voting with Ethereum blockchain

Kushal Chaganlal Choudhary
IT department, 3rd year
Pimpri Chinchwad College of Engineering, Akurdi
Pune, India

Saurabh Achal Agrawal
IT department, 3rd year
Pimpri Chinchwad College of Engineering, Akurdi
Pune, India

Mihir Manohar Gadhe
IT department, 3rd year
Pimpri Chinchwad College of Engineering, Akurdi
Pune, India

Mrs. Rohini Pise
IT department, Asst. Professor
Pimpri Chinchwad College of Engineering, Akurdi
Pune, India

ABSTRACT

When contrasted to the old methodology of pen and paper voting, e-voting decreased election costs and provided some convenience, but it was deemed unreliable since anyone with physical access to the system might impede the mechanism and alter the votes. A central framework is additionally necessary to control the whole strategy, from electronic voting through constituent comes about and following the results. Voters are not completely secure since their votes can be promptly focused on. It too postures a noteworthy threat to voting rights and openness. The purpose of this consider is to form a decentralized instead of centralised e-voting framework utilizing blockchain innovation, which guarantees voter personality security, information exchange security, and unquestionable status through an open and straightforward voting prepare.

Keywords—Blockchain technology, Decentralised System, Electronic voting, Ethereum, Secure.

I. INTRODUCTION

Elections are one of the basic cornerstones of any democratic society, since citizens vote for the most qualified candidate in order to build a healthy democracy. With technological advancements, the mechanical voting mechanism proved to be significantly more fluid, serviceable, and cost-effective, resulting in increased dependability and accuracy. Blockchain is a data structure that consists of blocks, each of which is linked to every other block via a chain. Each block contains information, a hash, and the past block's hash. In the event that the information in a block is adjusted, the hash of the block is additionally adjusted, be that as it may the taking after block will have the same unmodified hash as the going before piece, nullifying this block and all consequent blocks. This is to avoid tempering because changing one block requires calculating hashes for all subsequent blocks, but hackers can currently compute hundreds of thousands of hashes in a matter of seconds. To avoid this issue, it employs the proof-of-work idea, which slows down the formation of new blocks

II. Literature Survey

A variety of approaches have been developed to introduce differences in electronic and online voting systems, using various strategies and procedures. Despite the system's security to some level, voting continues to take place. Information and processes must be monitored and controlled that safeguards and protects the safety and privacy of voters and their information. Block verification using the Proof of Stake protocol does not require unnecessary computations. It's been implemented for Ethereum as well as a few other altcoins. Proof-of-stake methods partition stake blocks proportionally to the present wealth of miners, rather than proportionally to the relative hash rates of miners (i.e. their mining power).

Sr. no.	Name of paper	Authors	Technique used
1.	Survey on Blockchain Based E-Voting Recording System Design	Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao and Tuan A. Nguyen	AES algorithm
2.	Online Voting System	Vaibhav Anasune, Pradeep Choudhari,Madhura Kelapure and Pranali Shirke Prasad Halgaonkar	Homomorphic Encryption Technique
3.	Blockchain-Based E-Voting System	David Khoury,Elie F. Kfoury, Ali Kassem and Hamza Harb	Geth: Go-Ethereum
4.	Blockchain Based E-Voting Recording System DesignSr	G Bhavan	ECDSA(Elliptic Curve Digital Signature Algorithm)
5.	Decentralized Voting Platform Based on Blockchain	Friðrik Þ. Hjálmarsson , Gunnlaugur K . Hreiðarsson	HTML5 web-app compiled using Apache Cordova
6.	Votereum : An Ethereum-based E-voting system	Rifa Hanifatunnisa and Budi Rahardjo	External Personal Account(EOA)

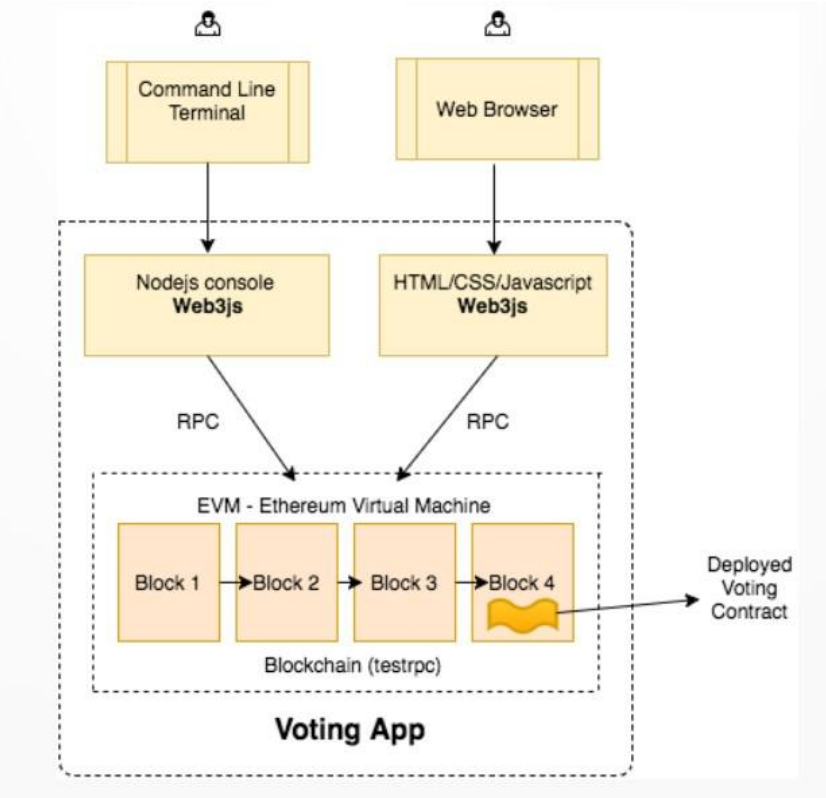
The theory behind Confirmation of Vote is that acquiring a sufficient amount of digital currency may be more difficult for miners than acquiring enough powerful computing equipment. The described polling method includes physical and logical verification of the voter and the voter's information. The tangible record of the computerised voting process can be verified (that is the national identification and biometric authentication) [Sravani C., Murali G, 2019].

Sr. no.	Factors	Ballot based systems	Electronic voting machines	Online voting systems	Our Blockckahin Model
1.	Fraud prevention	Average	Low	Low	Good
2.	Validity of ballot	Low	Good	Good	Good
3.	Vote tallying time factor	Extremely slow	Slow	Fast	Fast
4.	Cost factor	Expensive	Extremely expensive	Expensive	Less expensive on the long run
5.	Accessibility	Low	Low	Average	High
6.	Scalability	Low	Low	Average	High

III. Proposed System

A few apparatuses are utilized within the proposed framework, counting ganache, truffle system, npm, and metamask. Truffle imports shrewd contracts onto the blockchain, while ganache runs the inner blockchain, which can be available by metamask. A client must have a few Ether, or

Ethereum's cryptocurrency, in arrange to make an account with a wallet address. To compose a exchange to the blockchain, the client must pay a exchange charge known as gas.After votes are cast, the process is finished by minners, a group of nodes in the network. To finish the transaction, these miners compete with one another.The miners that succeed in this transaction are rewarded with ether, which is paid by users in exchange for their votes. For mining purposes, we shall use ganache software instead of nodes.



3.1 Preliminaries

Our proposed approach may be implemented with 64-bit hardware/machines, Windows 7 and later, NMP dependencies, Truffle framework, Metamask, solidity toolkit, and Ganache..

a) Dependency NPM(Node Package Manager)
b) Truffle framework
c) Ganache
d) Metamask
e) Coding language; solidity, HTML, JavaScript, CSS

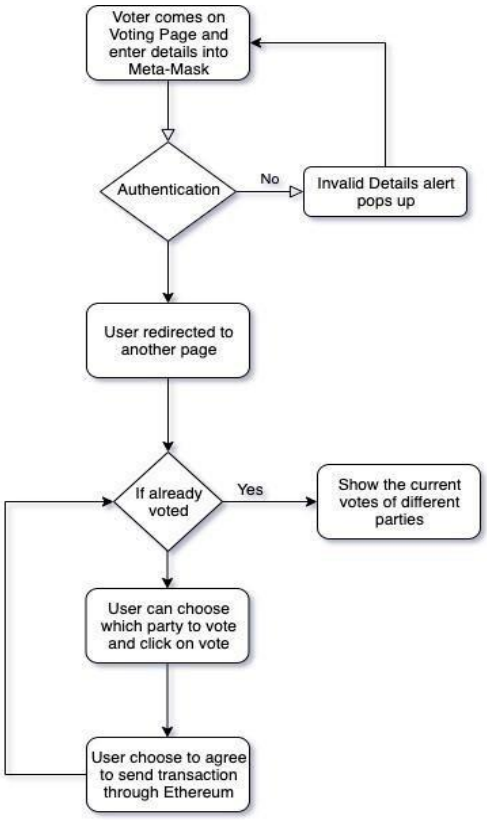
- **NPM (Node Package Manager) :**NPM is a package manager that allows you to manage, instal, update, and uninstall node.js packages in your project. It's a command-line programme. It has two modes of operation: local and global. All node.js applications are affected in global mode, but just a specific directory of an application is affected in local mode.
- **Truffle framework :**Truffle is a robust tool for interacting with Ethereum smart contracts. It is used for smart contract compilation, deployment, and linking, as well as providing a testing platform for automated contracts and managing networks and packages.
- **Ganache :**It was previously called as Testrpc and is available in both command line and graphical user interface versions. A fake blockchain creates ten regular Ethereum addresses,

each with its own private key and a simulated hundred ether. There is no mining with ganache; instead, it confirms each transaction automatically. It works with operating systems such as Windows, Linux, and Mac.

- **Metamask :**Metamask is an open source, user-friendly solution for ethereum transactions with a graphical user interface. Ethereal Dapps can work in your framework browser without requiring a full ethereum hub. Metamask is basically a connect between a browser and the Ethereum blockchain.
- **Solidity**: Solidity is a high-level language for contracts that uses JavaScript syntax. It's a way for converting EVM machinecode into basic instructions. It has the same operators as JavaScript, but it has four value types: Boolean, Integer, Address, and String.

3.2 Working of the system

After logging in to the voting website, the voter must use the Metamask Chrome Extension to connect to the local blockchain. The page is reloaded once the user is connected, and the user may see the candidates and current votes. Below that is the option to vote for a candidate; the voter selects the candidate and clicks on vote; a metamask pop-up appears, informing the user of the Ethereum transaction that must be completed; once the user clicks on Vote, the vote is given to the selected candidate, assuming the voter has not voted previously. A failed transaction will occur if the user has already voted and attempts to vote again. The vote will not be counted.



Flow model of the system

Ganache is utilized to form a local blockchain, and metamask is utilized to associate to it. The Truffle system empowers the movement of solidity-based smart contracts to a neighborhood blockchain.

Metamask permits clients to move Ether from one account to another when they vote. Each client is doled out a one of a kind ID, which is an Ethereum Address, a private key, and some Ethers are designated to each voter's account. When a client votes, Ether is moved from the voter's account to the Candidate's account, and all exchanges are handled through blocks. Once the extend is launched, all transactions will be available to everybody.

Metamask is used to connect to a local blockchain that was created with Ganache. The Truffle framework allows solidity-based smart contracts to be moved to a local blockchain. When voting, Metamask allows users to move Ether from one account to another. Every user is given a unique ID, which is an Ethereum Address, as well as a private key, and each voter's account is given an exact quantity of Ether. When a user votes, Ether is taken from the voter's account and credited to the candidate's account, and all transactions are carried out using blocks. All transactions will be open to the public once the initiative is launched [Hardwick, Freya Sheer, 2018].

3.3 Implementation and results

3.3.1 Setting up

The first thing we need to do is start up Ganache and run local blockchain. There will be no transaction after setting up ganache because we haven't done any yet (refer fig 1). By executing a command on the command line, we can now move the smart contract to the blockchain using the truffle framework. We've also used cmd to access the NPM directory. We start the project using the NPM directory using cmd after moving the smart contract (refer fig 2).

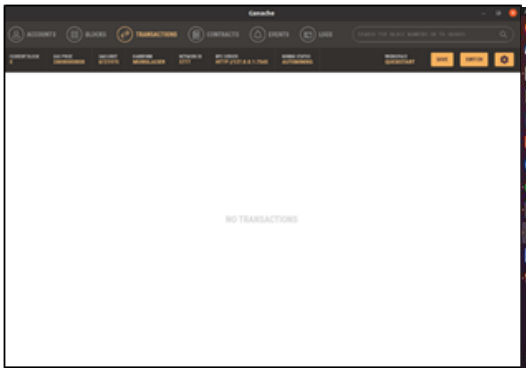


Fig. 1

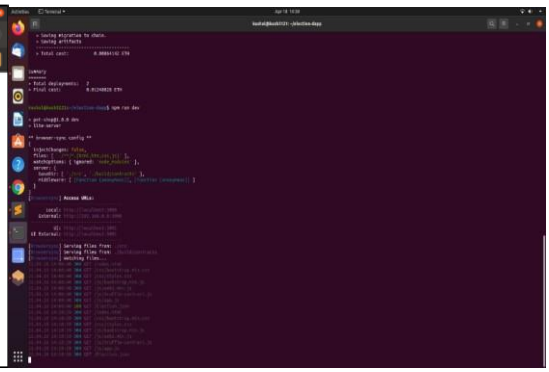
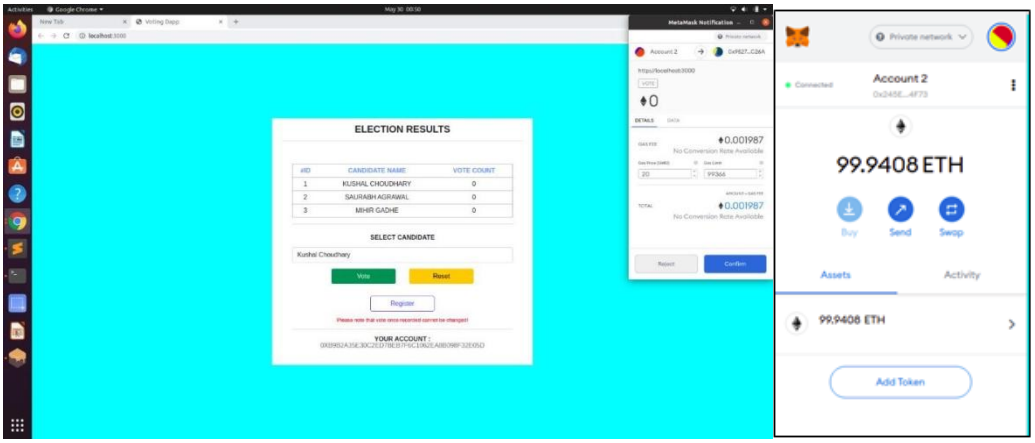


Fig. 2

3.3.2 User interface

Users engage with the e-voting system through the user interface. After logging in, the main screen appears with zero votes; the user is unable to vote until they import their account by inputting their private key.

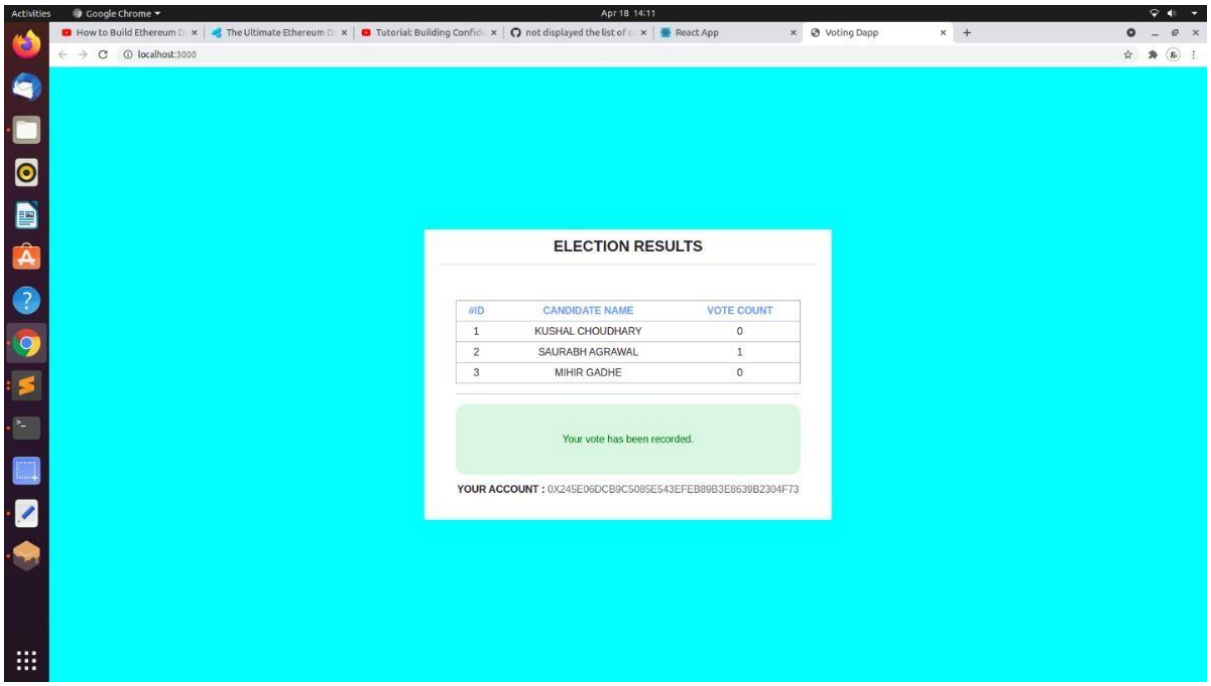


By entering the private key above, the voter imports their account. The electorate selects a candidate, and the metamask pop-up appears when the vote button is selected to finalise the transaction. After

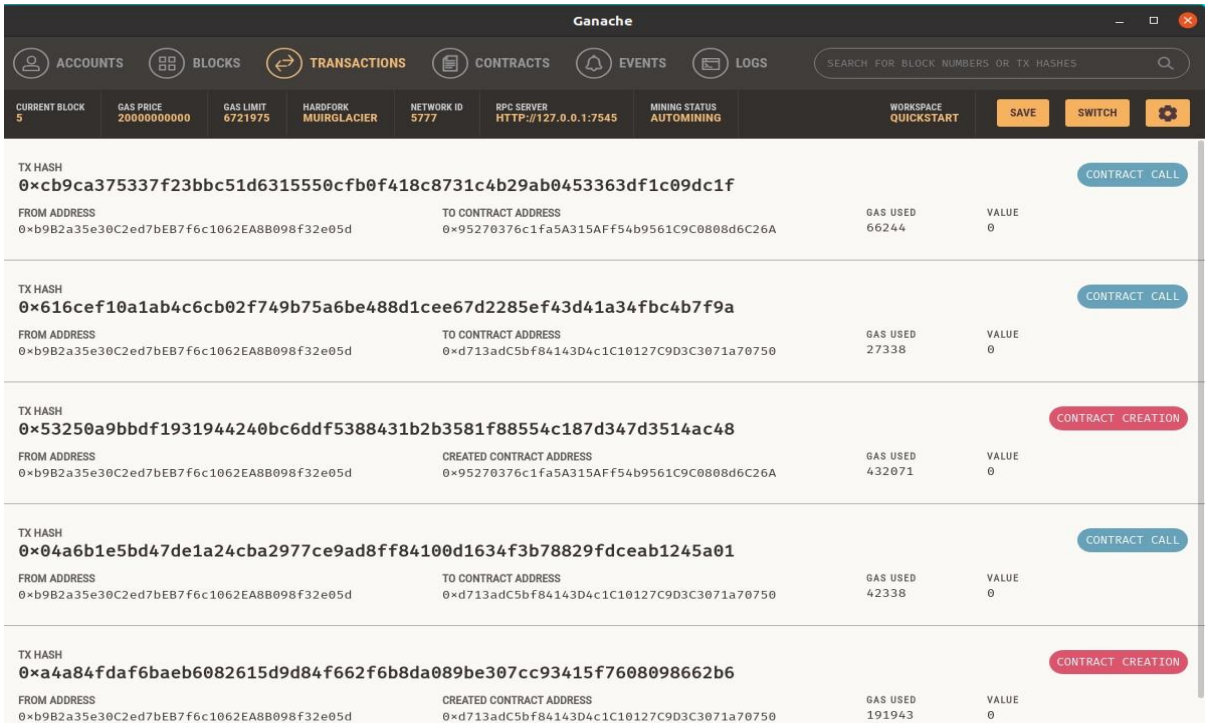
confirmation, the voter is taken to the main page, where just the results are displayed, but you can no longer vote. Others can vote in the same way by importing their accounts.

3.3.3 Checking the transactions

The transaction list will be made public to allow users to easily tally their votes.



By glancing at the transaction list, people can check the votes they've cast.



IV. APPLICATIONS

The blockchain records all exchanges (counting votes) in a disseminated record permitting open review of votes cast for a candidate, but the personality isn't uncovered. This permits freely irrefutable voting, whereas keeping up namelessness and avoids false votes. Investigate was in planning a framework is to permit voting beneath duress and uncovering a whole district's votes at the same time.

- Can be used in National Elections.
- Can be used in Television shows.
- Can be used in taking mass opinions.

V. CONCLUSION

Blockchain technology, a recent invention in the area of voting systems, has proven to be not only time and cost effective, but also safe and secure, making it more dependable and exact than previous techniques. We employed blockchain-based e-voting with smart contracts in this work, which feature a set of rules guiding communication and contract decision-making between participants. For implementation, many tools like as Ganache, Truffle framework, NPM, and metamask were utilised.

Seeing as blockchain technology is decentralised, it is very easy to temper and change such a system. Our proposed solution gives voters convenience by allowing them to connect to a system with an easy-to-use user interface, which allows them to cast their vote by importing their account and easily evaluate their vote. It instils confidence in voters by ensuring that their votes are counted and stored securely.

REFERENCES

[1.] Zhang,S., Wang, L. &Xiong, H. Int. J. Inf. Secur. (2019) Chaintegrity: blockchainenabled large-scal e-voting system with robustness and universal verifiability. International Journal of Information Security.

[2.] Gjøsteen K, Lund AS (2018) An experiment on the security of the norwegian electronic voting protocol. Annals of Telecommunications:1–9. doi:10.1007/s12243-016-0509-8

[3.] Rashid Hafeez Khokhar, Md Asri Ngadi& Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, vol (2) issue 3.

[4.] Venkata Naga Rani B, Akshay S, Arun kumar M , Ishwar Kumar M A , (2019) , Decentralized E-Voting System,International Research Journal of Engineering and Technology

[5.] Vaibhav Anasune, Pradeep Choudhari , Madhura Kelapure and PranaliShirke Prasad Halgaonkar,"Online Voting: Voting System Using B-chain",(2020), Online Voting: Voting System Using Blockchain

[6.] Sravani C., Murali G. Secure electronic voting using blockchainand homomorphic encryption. International Journal of Recent Technology and Engineering (IJRTE), vol. 8, 2019, p. 1002-1007

[7.] Shaheen S. H., Yousaf M., Jalil M. Tamper proof data distribution for universal verifiability and accuracy in electoral process using blockchain. 13th International Conference on Emerging Technologies (ICET)

[8.] Hardwick, Freya Sheer, et al. "E-voting with blockchain: An e-votingprotocol with decentralisation and voter privacy." 2018 IEEE International Conference onInternet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) andIEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

[9.] Alharby, Maher, and Aad van Moorsel. "Blockchain Based Smart Contracts : A Systematic Mapping Study." Computer Science & Information Technology (CS & IT)