Journal of Current Research in Engineering and Science
JCRES
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7-Issue 1, January 2024

Paper: 51

E-Voting System using Blockchain

Arjun Adhikari[1], Aftab Khan[2], Ritik Kumar Roy[3], Akash Bhasney[4]
[1,2,3,4]Department of Computer Science & Engineering
School of Engineering and Technology
Sharda University, Greater Noida, India

***Abstract*—Traditional elections fulfilled neither citizens nor political authorities withinside modern years. They at the moment are not absolutely steady as it is simple to attack votes. It moreover threatens the privateness and transparency of voters. Additionally, it takes an immoderate amount of time to rely on the votes. We recommend a Blockchain-based totally complete solution for solving various troubles faced within the balloting process. This task is a smooth try to format and construct an electronic voting system; in which we rent Solidity Smart Contracts to create a decentralized balloting application (DApp). Our implementation consists of a net interface to allow customers to interact with the blockchain, and rest API to cope with the specified records information. For a private blockchain, we've got used a go-based totally completely Ethereum implementation. Blockchain technology is a disruptive generation of the cutting-edge era and ensures to decorate the general resilience of e-voting systems. Blockchain technology presents a countless variety of applications taking advantage of sharing economies. This paper goals to assess the software of blockchain technology as a provider to implement distributed electronic voting systems.”**

Keywords— Blockchain, Ethereum, Smart Contract, Evoting, MetaMask, Ganache, Truffle Framework

I. INTRODUCTION

In this World, The security of the Election Matters for the National Security. Elections are the pillar of the Democratic System to express the vote. Many more Research has been done on the Electronic Voting System which enables the voters to vote by using their own setups like Computer, Laptop, Mobile and other electronic devices. Still, none of these technologies have been produced in a large amount So that the people can cast a vote.

Entering in the block chain Technology, it was introduced in 2008 when Satoshi Nakamoto created the first Cryptocurrency Called Bit coin. A block chain is assets one of the digital assets with Emerging, And Immutable Technologies with strong Cryptographic Foundations. The block chain is considered as a Type of payment rail. The Major use of the Block chain has been in all Crypto currency transactions, mainly in a Bitcoin [1]. A block chain collects all the Data structure which maintains and shares all the Transactions which is being accomplish by its Genesis. Block chain allows every new user to connect to the network, Send the new Transitions to it, Verifies the Transactions and create new Blocks.

E-voting, is a significantly new idea that permits voters (citizens) to vote online thru particular internet portals and cell applications. On the opposite hand, it is nevertheless now no longer widespread It removes the want for dispensed vote centers, paper ballots, ballot containers, and observer personnel. Hence lowers the charges significantly. However, it is nevertheless not often getting used because the number one manner of amassing people’s picks and reviews no matter the subject.

Blockchain is a community and a database all in one. A blockchain is a peer-updated-peer community of up-to-date structures, referred upupdated nodes, that proportion all of the information and the code withinside the network. So, if a device updated is attached updated the blockchain, then the node is withinside the community, and moreover, speaks with all the one of a kind up-to-date nodes withinside the community. Now a duplicate of all of the records and the code is at the blockchain. There aren’t any more essential servers. just a organization of up-to-date machines that speak with every one of a kind withinside the equal community. all the transaction statistics that is shared at some stage in the nodes withinside the blockchain is contained in bundles of facts up to date blocks, which is probably chained upupdated create most of the people contemporary. This public modern represents all of the data withinside the blockchain. All the facts withinside the general public present day are secured thru cryptographic hashing and installed via a consensus set of rules. Nodes within the network take part up-to-date ensure that everybody copies of the statistics allocated throughout the network are equal. That’s one very important cause why e-voting programs built at the blockchain, as it guarantees that vote is counted, and that it did now not alternate.

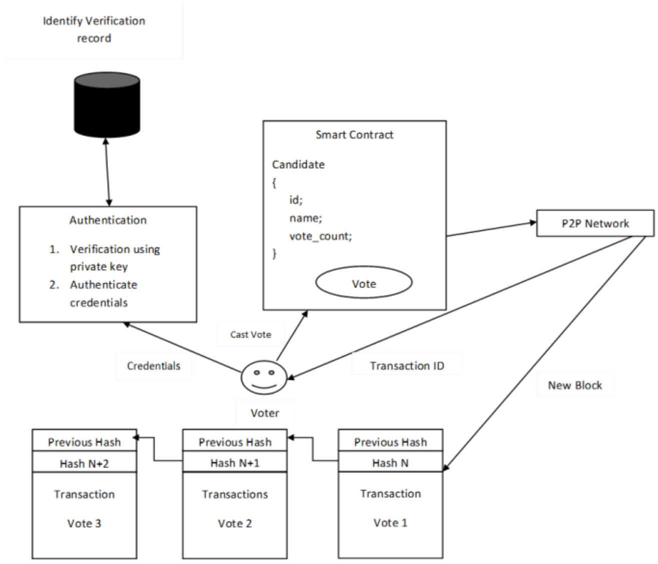


Fig-1 Voting Process

II. LITERATEURE REVIEW

This section presents some modern-day e-voting systems that use blockchain technology. Reviewing the literature shows that blockchain technology based totally solutions had been proposed for voting in businesses, agencies, and states.

In2014, in Russia, the metropolis of Moscow's lively Citizen software turned released [4]. Many polls had been performed given that then on several up-to-date like what wishes updated be the shade of seats in an emblem-new sports activities area, etc. [5]. In2017, in South Korea a smart contract-up to date blockchain-enabled the vote casting device up-to-date used [6]. all of the vital records like votes and effects up to date updated up-to-date on a blockchain. There up-to-date no involvement of any vital authority or manage in the process.

AliKaan Ko et al. talk in their paper entitled" closer up updated comfortable E-balloting using Ethereum Blockchain" [7] a decentralized vote-casting solution based up updated up-to-date Ethereum Blockchain. It states that an E-vote casting up updated need up updated be regular thru way of approach of being absolutely obvious (privatenessconscious) and now not permitting duplicated votes. It shows deploying the E-balloting application as a clever agreement and permitting updated with valid EOAs up-to-date vote on that settlement (as soon as updated address a unmarried question). despite the fact that, this solution lacks a proper automatic deal with a verification protocol for the purpose that EOAs get their right vote from a Centralized Authority updated up-to-date eligible electorate. the foremost benefits it gives are company guidelines transparency and single vote limit consistent with EOA.

In 2018, Agora that is Swiss blockchain startup advanced a blockchain-based balloting machine. It became partially tested in 2018 Sierra Leone's standard elections [8]. Agora is a quit-updated-up-to-date verifiable blockchain. Itis designed up-to-date provide a web balloting gadget updated corporate, governments, and establishments. This blockchain-up-todate up to totally e-balloting system gives an up-to-date token device, wherein the institutions or the authorities purchases up to date tokens for eligible voters.

In2017, McCorry et. al. proposed a Boardroom voting with maximum Voter privacy [9]. It makes use of a clever contract updated offer a self-tallying balloting protocol. This blockchain-up to date decentralized Open Vote community (OVN) is built upon Ethereum.

In2018, Jonathan et. al. introduced Net vote [10], a decentralized blockchain technology primarily based on balloting machine. It is primarily based totally on the Ethereum community and uses decentralized application (dapps) for the personal interface. Three dapps are introduced by the authors. First one is the admin dapp, that's for control to set guidelines and regulations, etc. Second dapp is Voter dapp used by personal customers to sign in and vote. And the last, Tally dapp issued to tally and claim election results. However, this machine is primarily based totally on the personal blockchain technology.

III. HOW DOES BLOCK CHAIN WORKS

Blockchain mainly consists of three important Concepts:

Blocks, Nodes and Miners.

1) Blocks:-

Blocks in a blockchain is a document wherein the information is carried out to the community of bitcoin and are lifelong recorded. Thus, the block withinside the blockchain is just like the web page of a Balance sheet or, Record book. The block stores the record completely and cannot be altered or, removed. A block in a blockchain represents the 'present' and carries the Information and Data approximately its Past and the imminent Future. Each time while a block is finished and turns into part of the beyond and it allows to offer a manner to shape a brand-new block in a blockchain. The finished block is an everlasting document of the transaction withinside the beyond in a blockchain and the brand-new transactions are recorded withinside the present-day one which allows the growth of the blocks withinside the blockchain. As we are able to address the instance that if we do any transaction with the ATM or, Bank. They record it which cannot be modified or, deleted. Each block withinside the blockchain carries a variety of transactions, Each and whenever a brand-new transaction happens withinside the Blockchain, all of the records of the Transaction Are Recorded withinside the

Participant's Record book.

2) Miners:-

The Miners are those who help to create the new blocks on the blockchain by the process called mining. "In blockchain every block has its own Unique Nonce (A 32- bit Whole number) and Hash (256- bit number wedded to the nonce) So mining a block isn't Easy, especially in a large chain". In the ledgers, the block chain miners help to protect the blocks and get connected to each other to form a chain and it still takes 10 Minutes to mine one Bit coin. The miners use the special types of software which helps to solve the extremely complex mathematics problems for detecting a nonce which can generate an accepted Hash, because "the nonce has only 32 bits and the hash has only 256 bits". After that when the blocks in a blockchain is successfully mined, the change is accepted by all of the nodes from the network and finally the Miner Are honored financially.

3) Nodes:-

A node of the blockchain is an opens source cross platform that allows the developers to create the various services in the blockchain. Nodes may be of any kind of the electronic device that maintains the copies of the blockchain and keeps the network functioning. Since, Block chains are Clear/Transparent, Every Actions in the financial book can easily been viewed and checked. Every Participants in a block chain has got a unique alphanumeric identification number which allows their participants to see their own Transactions. The p2p (Pear to pear) protocol allows the nodes to communicate with each other in the network and also helps to share the information of the Transaction in the blocks. These nodes can communicate with each other by Storing and Updating the information. Mining a node aren't actually responsible for maintaining the blockchain, Instead they are only responsible for creating the blocks to add to it and after that when the blocks are created, it is sent over the network to full the nodes which justify them and after that they are added to the Blockchain, which provides the users trust via technology.

IV. IMPLEMENTATION DETAILS OF BLOCKCHAIN BASED EVOTING

For the implementation of the block chain, we decided to use the Ethereum block chain as it is one of the open sources, safe and widely used platform for developing and for establishing the Applications in the market.

A. Layoutu Inspection:

The given point is the important one and also should be Reviewed/Examine while implementing the e-voting system:

- At first, the electronic voting system should verify the identity of the voters and match the fingerprint and then only allow them to cast a vote.
- Secondly, the electronic voting system should not permit the Access to the invalid Candidates to cast a vote.
- Each and Every Voter should get only one chance to cast a vote.
- It should provide the total security and the privacy to the voters who comes to cast a vote.
- They should not be allowed to Alter the Votes which was Casted by the voters during Voting.
- The system should allow More than one or, multiple control on counting the Casted Votes.

B. Ethereum

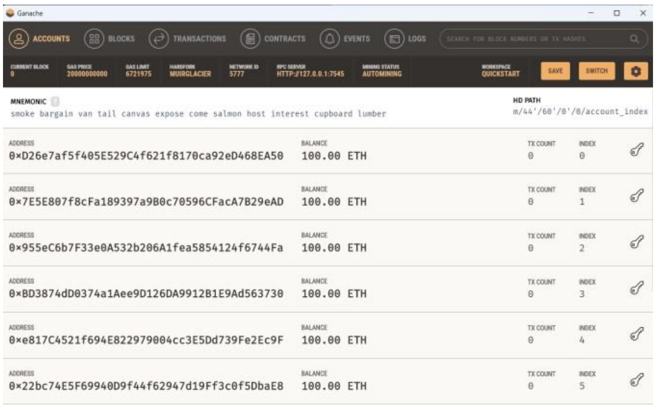
Ethereum is a public Distributed Block chain with smart contract network. Basically, Ethereum is the technology that is made for digital money, global payments which allows the programmers to build the distributed applications using the block chain technology. The community has built a strong Digital money which helps the creator to earn online. It's open to the every one, any people can operate and can earn, and all you need is the internet for operating [1]. Ethereum helps to provide the wide range of the services and the path to the development tool and the smart contract. A smart contract is a self-enforcing computer program or, a transaction protocol that runs automatically on the block chain when the predetermined conditions are met. They are runes on the block chain, so they are stored on public data Information and cannot be changed. The block chain also helps in processing the transactions happen in the smart contract, which means that they can also Dispatch automatically without the help of third party. The currency which is required in smart contract to execute it is called "gas amount" and the help of third is varies from "contract to contract" as p2p (pear to pear). In the Ethereum block chain nodes are operated in the real time, which confirms that every transaction that happens in a blockchain is totally confirmed and verified by all the given nodes or, No nodes at all [1].

C. Smart Contracts

The smart contract is the self-executable code that is written in the blockchains. These are alike to Standard organization contracts which might be used as code of behavior agreements between the two group. The smart contracts are executed automatically when the described situations are matched. Smart contracts assist to perform the agreements and the transactions in a relied-on way for some of the unknown parties without the requirement of the central authority [3].

The Programing language that we use is Solidity which immediately runs on the Blockchain. Solidity is extensively utilized in Smart contract for writing. The Contracts which might be achieved with the aid of using all of the nodes and proportioning the up-to-date data to some other node after every normal interval. To get activated those contracts need to be tested with the aid of using 2 nodes. Even though the Ethereum blockchain technology is unfastened to apply to the public but, it expenses ether for nodes to put into effect on the smart contract. This cost of the Ether referred to as gas. In Ethereum, gas works at the smart contract with its functions. The smart contracts additionally don't want the evidence of its work as every node of the blockchain will carry out the transactions with the Smart contractor, not. Since the primary network of Ethereum offers Actual Ethereum that's Very costly and right here we used our personal Ethereum test network that's called the truffle network. The checking out framework that's extensively used for Ethereum is Truffle which facilitates making it easy to set up and execute the smart contracts at the Ethereum blockchain. It additionally facilitates us with the aid of using imparting a choice to set up a public or, a private blockchain community.

The Ganache software is a part of the Truffle ecosystem. While working with the Ganache, it gives a graphical environment to us. It provides us ten accounts with one hundred ETH each which help to make it easy to establish and perform the Network transactions in the blockchain. Election contract has all the Module that we require in our smart contract. If we have to define each nominee standing in the election, we are using a complex data type structure which has the candidate's ID, with Name and his vote count.



CURRENT BLOCK 0 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE QUICKSTART

MNEMONIC
smoke bargain van tail canvas expose come salmon host interest cupboard lumber

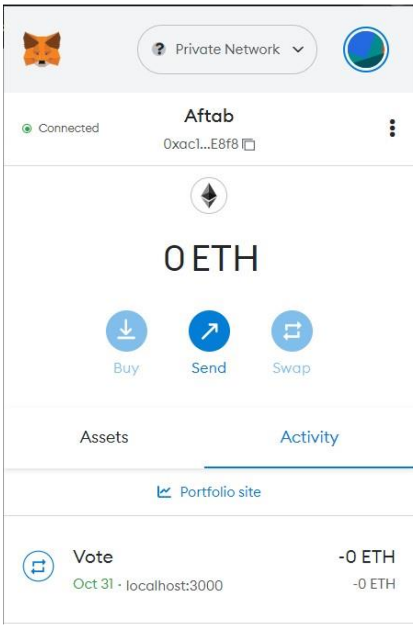
HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×D26e7af5f405E529C4f621f8170ca92eD468EA50	100.00 ETH	0	0
0×7E5E807f8cFa189397a9B0c70596CFacA7B29eAD	100.00 ETH	0	1
0×955eC6b7F33e0A532b206A1fea5854124f6744Fa	100.00 ETH	0	2
0×BD3874dD0374a1Aee9D126DA9912B1E9Ad563730	100.00 ETH	0	3
0×e817C4521f694E822979004cc3E5Dd739Fe2Ec9F	100.00 ETH	0	4
0×22bc74E5F69940D9f44f62947d19Ff3c0f5DbaE8	100.00 ETH	0	5

Fig-2 Ganache

Once the nominee is announced, applicants want to speak to the citizens in order that one voter can most effectively vote for a single nominee. Then, all of the voted accounts want to be stored, in addition to a variety of Nominees who're withinside the election. Finally, we want to check and provide the permission to vote for the most effective the ones who nonetheless must solidify vote. To attain this, an occasion with the intention to most effectively permit a voter to cast a vote for once.

To perform the voting, customers want to pay for a small quantity of gas. This gas charge also can be performed in a couple of ways. Metamask is the only manner getting used right here and is likewise an extension for the Mozilla Firefox or, Google chrome. Metamask facilitates us to go to the distributed blockchain thru our browser and run Ethereum smart contracts without running on the complete Ethereum nodes. "This is best for the app right here due to the fact it's miles only worried about the voting app and now no longer with the alternative heavy transactions on the blockchain". To solidify a vote on the usage of metamask, we should make an account and connect with the check community about the usage of our given Ethereum address.



Connected
Aftab
0xac1...E8f8

0 ETH

Vote -0 ETH
Oct 31 · localhost:3000 -0 ETH

Fig-3 Metamask

The part of the Truffle ecosystem is Ganache. It provides Ethereum development with a private blockchain which also can be visible as an Ethereum customer. Ethereum customers also can be used to check the decentralized software which is constructed on the truffle. It may be used to install contracts at the same time as evolving decentralized applications. It additionally permits us to run assessments on blockchain and smart contracts. Ganache is the framework of our desire wherein its miles powered via way of means of truffle and has 10 accounts with one hundred ETH every to work with [2]. To connect to this community, Ganache has begun out then the deal with supplied in Ganache is open source on our browser of desire. Once the web page loads then, log in to the metamask account and connect with the test network running on.

A fraction of ether as gas amount is used for voting on the blockchain. As soon as the transaction occurs, the gas is used and all other nodes are informed about this transaction as well so the voting occurs in real time and becomes difficult to tamper with it.

V. CONCLUSION

This paper indicates decentralized e-voting system up-todate on blockchain that operates on Ethereum. Our principal intention of decentralizing the transactions going on with the voting device has been carried out with its software and we succeeded in securing the privateness of the citizens. This implementation makes us use of smart contracts. In future, this application may be developed similarly updated make it greater eligible and comfy for the government election, based on fingerprint.

VI. REFERENCES

[1] Ethereum project: https://ethereum.org

[2] Canessane, R. Aroul, et al. "Decentralised applications using ethereum blockchain." *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*. Vol. 1. IEEE, 2019.

[3] Patidar, Kriti, and Swapnil Jain. "Decentralized e-voting portal using blockchain." *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019.

[4] M. Hochstein, “Moscow’s Blockchain Voting Platform Adds Service for High-Rise Neighbors,” CoinDesk, 15 Mar. 2018; https://www.coindesk.com/ moscows-blockchain-votingplatform adds-service-for-high-rise-neighbors, 2018.

[5] M.D. Castillo, “Russia Is Leading the Push for Blockchain Democracy,” CoinDesk, 2018; https://www .coindesk.com/russias capital -leading-charge-blockchain–democracy, 2018.

[6] “South Korea Uses Blockchain Technology for Elections, ”KryptoMoney, https://kryptomoney.com/ south-koreausesblockchain-technology-for-elections, 2017.

[7] A. K. Koc¸ and U. C. C¸ abuk, “Towards secure e-voting using ethereum blockchain.

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

[9] Patrick McCorry, Siamak F. Shahandashti and Feng Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy”, Published in: Financial Cryptography and Data Security, Springer, 2017.

[10] Jonathan Alexander, Steven Landers and Ben Howerton, “Netvote: A Decentralized Voting Network”, https://netvote.io/wp content/uploads/2018/02/Netvote-White-Paper-v7.pdf, 2018.

[11] Truffle: https://truffleframework.com

[12] Ganache: https://truffleframework.com/ganache