IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

Ether Ballot

Tejashwini N[1], Aadhya Singh[2], Vaishnavi Jaiswal[3]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3]
Sai Vidya Institute of Technology Bangalore, India
tejashwini.n@saividya.ac.in, aadhyasingh2000@gmail.com, vaishujais1601@gmail.com

Abstract: *Digital technology is currently helping many people. In contrast the electoral system, there is a common use of paper in its implementation. National elections are still using the middle system in which there is one organization in charge. Some of potential problems with traditional electoral systems are associated with an organization with full control over the database and system, it is possible to disrupt a multi-opportunity website. As a solution to it blockchain technology can be implemented with feature of decentralization which means the data are not stored at a particular organization. This discusses E-voting system using blockchain algorithm.*

Keywords: E-voting.

I. INTRODUCTION

Vote casting is extensively used in society. The protection and privacy are constantly the crucial characters. within the vote casting system, a number of people make their choices which can be saved secretly. Most of the e-voting schemes relies on public bulletin board to provide a constant view to all citizens. Blockchain may be used as the bulletin board because the content is publicly trusted.

Blockchain served as a decentralized database that provides new gear for growing trustless and decentralized device. inside the blockchain gadget, no data relies on a centralized co-ordinator. rather, every node that is involved inside the blockchain gadget holds the statistic block locally. Blockchain is maintained with the aid of a decentralized and open-membership peer to see network. Researchers are looking to reuse Blockchain in other research regions which include coordinating the internet of things, carbon dating and health-care. This sparked the invention of Ethereum, that's properly called a milestone inside the development of blockchain.

Blockchain can be trusted by the public. In addition to it the implementation of smart contracts adds an advantage overall.

The vote casting protocol is deployed on Ethereum through smart contracts. The Ethereum script allows customers to write down the desired smart contracts on Ethereum and enforce powerful functions through it to implement decentralized programs. All nodes of Ethereum network run the code independently to ensure the credibility of the final end result. The final result is public verifiable.

II. METHODOLOGY

2.1 Working of a Blockchain

A blockchain encompass blocks preserving information arranged in a sequence. Blockchain is basically a ledger distributed over the network. Blockchain has a robust structure of related list that is immutable. each block has some records, hash of previous block and hash of itself. A block also has a hash, you can examine a hash to any sort of bio-metric price. The contents of the block are continually unique. once the block is being created, the hash is being calculated. Any amendment with the block will change the data for other hash as well, as hash is the critical a part of the blockchain. The 1/3 element interior a block is the hash value of the preceding block. This effectively creates a chain of blocks with every block pointing preceding block and therefore making it computationally not possible to mutate any block.[1]

In the figure above we can see there are three blocks. each block has a hash and hash of the preceding block. The third block points to second block and the second block points to first block. the first block is referred to as the Genesis block. Tampering with any of the blocks will motive an exchange within the data of hash due to which the complete chain might be compromised.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

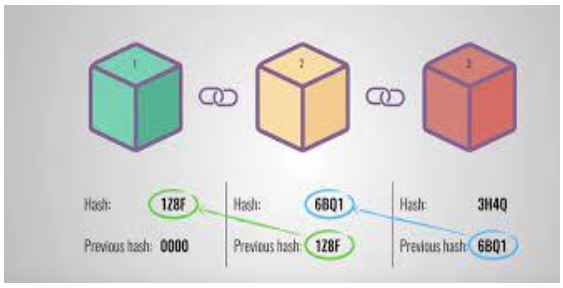

Figure 1. Basic blockchain diagram

Safety of Blockchain comes from its innovative hashing and the evidence-of-work mechanism. One more way that blockchain secures itself is with the aid of being distributed. Instead of using a central entity to manage the whole data blockchain uses a peer to peer network and each peer is allowed to join, when someone joins the community they get a full proof replica of the blockchain. The node can use this to check that the entirety is in right order and nothing is tampered. when someone creates a new block. The block is despatched to each peer in that specific network. each node then rectifies the block to make positive that it has not been altered. As soon as the verification is completed by means of all of the nodes then a consensus is generated. so to tamper blockchain, all of the blocks in the chain want to tamper which is not viable via any manner of computational strength.[1]

The blockchain also consists of an interesting concept of smart contracts which has different forms of application in blockchain. While using Ethereum, smart contracts needs to be implemented.

III. LITERATURE SURVEY

1) Paper titled "**A Smart Contract For Boardroom voting with Maximum Voter Privacy**" had propose the net voting protocol with decentralized features and maximum voter privateness using the Open Vote network (OVN). The OVN is a smart settlement for the Ethereum Blockchain. After imposing this system the creators concluded that it prices 0.73$ consistent with voter in this system. They had an upper limit for the number of voters to50 to reduce the gas usage but, the researchers soon discovered out that OVN is liable to DOS assaults. It can also go through via site visitors jams in the course of the transaction that could postpone the balloting procedure for a longer time, Therefore this implementation is a success for boardroom meetings with a major drawback that every character who desires to vote needs to download the complete reproduction of the network.[2]

2) Paper titled "**Trustworthy Electronic Voting Using Adjusted Blockchain Technology**" This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.[3]

3) Paper titled"**"Votereum: An Ethereum-based E-voting system**" proposed Votereum, an Ethereum-based totally E-balloting machine that makes use of blockchain generation and smart contracts to permit an open, cozy election whilst protective voter's privateness. The paper mentioned the requirements, architecture, design of the machine and an actual-existence scenario of cited voting scheme. The system has fulfilled the primary requirements of poll privacy, uniqueness, commonplace verifiability and robustness but, it does no longer satisfy the desires of receipt-freeness and coercion-resistance. By way of using the proposed balloting scheme, citizens are allowed to be tested and vote at their close by resident election station which could doubtlessly growth voter turnout.[3]

4) Paper titled "**Blockchain for Electronic Voting System Review and Open Research Challenges**" The purpose of this study is to research and compare current research on blockchain primarily on based digital vote casting systems. the item discusses latest digital vote casting research and the use of blockchain generation. The blockchain concept and its uses are presented, followed by existing electronic voting systems then, a fixed number of deficiencies in existing electronic voting structures are diagnosed and addressed. The blockchain's potential is essential to enhance digital voting, current solutions for blockchain-primarily based electronic voting, and possible research paths on blockchain-based totally digital voting structures. The paper also says that adopting blockchain balloting methods can also divulge users to unforeseen security risks and flaws. Blockchain technology require a more sophisticated software architecture as well as managerial expertise.[5]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

5) Paper tilted "**Secure Digital Voting System based on Blockchain Technology**" focuses on the study to analyse the important issues consisting of voter anonymity, vote confidentiality and end to end verification. These challenges form the inspiration of an efficient voting machine retaining the integrity of the voting method. This paper presents the efforts to explore using the blockchain technology to search for solutions to these demanding situations. It affords an attempt to leverage benefit of blockchain including cryptographic foundations and transparency to achieve an powerful scheme for e balloting. The proposed scheme conforms to the essential necessities for e-balloting schemes and achieves end to end verifiability. This paper offers the implementation of a system with the usage of Multichain platform and additionally in-depth evaluation of the scheme which efficiently demonstrates its effectiveness to obtain an give up-to-stop verifiable e-voting scheme.[6]

IV. ETHEREUM- A BLOCKCHAIN PLATFORM

For developing the E-voting using blockchain we are using a platform called Ethereum which is a popular platform for creating distributed blockchain application that supports smart contracts. Ethereum, additionally referred to as world computer is a blockchain platform used to construct decentralized programs in which every software and motion is universally on hand and verifiable as it is available on the global Ethereum community. Ethereum is a global allotted ledger where all agrees to run the same program and records, subsequently it miles a global shared processing protocol. To lessen spams and disincentive valueless transactions, we require gas that is ether in case of Ethereum.[7]

But it's impractical to expect all people to have a duplicate of the complete blockchain community. So the blockchain network has delivered concepts like blockchain servers, metamask, and many others wherein you need not invest heavily in RAM and disk area and on the same time maintain decentralization.

There are two components in blockchain:

1) Database: All transactions within a blockchain network are saved in blocks. While an application is deployed it is considered as a transaction. In the case of our voting system, every vote being cast is counted as a transaction. these transactions are public and are available for verification, so to make certain that all nodes within the network have the same records copy and no invalid records is written to the network, blockchain makes use of an algorithm called 'proof of work'.

2) Data: the software code is written in the form of contracts within the Solidity programming language. Solidity compiler is used to assemble it to Ethereum byte code and this byte code is deployed to the blockchain.

Some terms related to Ethereum:

1) Smart contracts: These are self-executing contracts which contain the terms and conditions of agreement between peers. They are simply programs stored on a blockchain that run when predetermined conditions are met.

2) Ether: Ether is the native cryptocurrency of the platform.

3) Address: Address is the identity on the network which is in the form of 001d3f2efe111827442a40 27bd3hgf1f086ba0f8 associated with a primary key.

4) Gas, Gas price and Gas limit: Gas is the amount of work done in the transaction. Each unit of gas has a price associated with it. This is se in the gas price field. Since we do not know the amount of ether that will be consumed in a transaction, we specify a limit on the maximum gas units we are willing to spend on a transaction. This is called the Gas limit.

5) Ethereum virtual machine: it's far a easy, powerful 256-bit Turing machine capable of strolling EVM Bytecode. EVM is a part of the Ethereum system and it is critical in consensus engine. whenever you run the consumer or browser, the EVM starts to sync, validation, and execution of transactions.

V. IMPLMENTATION

5.1 Frontend

React- It is a JavaScript library for building use interfaces. Our whole project is build on react from user signup to displaying voting results. React is integrated with web3.0 in order to do voting transaction connected with our Ethereum wallet i.e. MetaMask.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

MetaMask- It is as software crypto-currency wallet used to interact with Ethereum blockchain. This wallet can contain multiple accounts secured by 12 words secret key. In order to do voting user has to select desired account along with gas fee(which determines the speed of transaction) to process transaction on Ethereum nodes.

Web3.0 – It is a technology which revolves around decentralisation and token based economic. It helps in connecting user to blockchain space. It consists of many kinds of blockchain (bitcoin, solana, Ethereum, etc.). We are using Ethereum blockchain which works on Proof-of-Work (PoW). In order to make user vote it will connect user node to other ethereum nodes. Thus it acts like a bridge between frontend and Ethereum blockchain.

API's-To fetch the data from the backend and to display it on our users on frontend API's are used. We are using many API's depending upon the action performed by the user on the website

5.2 Backend

Node – In order to make the website dynamic and authentication, we are using single-threaded, event-loop based nodeJs. Authentication and authorization is done by JWT(JSON web token), which make sure the person who is interacting with API's is genuine. It also controls unauthorised actions such as voting time period. It maintains users sessions based on users time period token, which means after certain period of time user will be again authorized.

Database – We are using Mongodb as our database which works on NOSql .It holds different kind of user data(Electoral party, voter and admin).Data of other features of the website such as blogs, announcements, voting related data.

VI. ETHEREUMS'S BLOCKCHAIN

Smart Contracts – These are written in solidity language which acts as self-executing contracts with the terms of agreement between two parties(as per our project it's between voter and admin of election).Once they are deployed they can't be changed and if changed it will be known to others. Thus, this forms the base of trust for the voters. Our voting Smart Contract checks following things :- a) if user is voting more than once. b) the election party to whom the voter is voting is registered. c) whether voter is voting at legmit time i.e during the given duration of voting period only. If any one of the condition is not satisfied vote of that particular voter will not be considered. Smart contract is responsible for showing the result of the election to anyone once the voting period is over.

Ganache & Truffle – To do any kind of transaction on blockchain gas fee is required which costs real money. So, we are building our personal Ethereum building network where we deployed our smart contract with help of ganache. Truffle on the other hand is completely a development , testing and asset pipeline environment specifically for Ethereum blockchain. Thus, ganache and truffle work together for local development phase.

Remix Solidity – It is used in development phase of the project where we deployed our smart contract and done regression testing on them, by checking if the specified conditions are met in order to do voting and showing election results.

VII. CONCLUSION

Online voting is the future because everything geared toward easy usability for the user. online vote casting is the destiny due to the fact everything geared towards easy usability for the give up consumer. The goal of building an E-voting scheme using blockchain technology is to make the electoral technique quicker, easier while lessen the price of conserving a conventional election. It also ambitions to take away the existing security concerns of the contemporary conventional voting scheme. The maximum essential difficulty is the trust issues between voter and election authority. with the aid of adopting blockchain advantages, the need of trust in individuals may be minimized due to the fact blockchain operates beneath no control of single entity.

In this paper, we proposed Ether ballot, an Ethereum-based E-vote casting machine that utilizes blockchain era and smart contracts to permit an open, relaxed election while protecting voter's privacy. The proposed system has fulfilled the requirements of ballot privateness, forte, standard verifiability and robustness.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

REFERENCES

[1]. S. Haber and W. S. Stornetta, "How to time stamp a digital document," in Advances in Cryptology-CRYPTO' 90, A. J. Menezes and S. A. Vanstone, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 99–111.

[2]. P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[3]. Trustworthy Electronic Voting using Adjusted Blockchain Technology P. Raghava1 , P. Uday Kiran2 , Vimali. J. S3ISSN 2321 3361 © 2020 IJESC Volume 10 Issue No.5.

[4]. Votereum: An Ethereum-based E-voting systemLinh Vo-Cao-; Cao-Minh, Khoi; Dang-Le-Bao, Chuong; Nguyen, Tuan A. (2019). [IEEE 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF) - Danang, Vietnam (2019.3.20-2019.3.22)]

[5]. Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874. https://doi.org/10.3390/ s21175874

[6]. Secure digital voting system based on blockchain technology Kashif Khan Junaid Arshad Muhammad Khan1 May 2018.

[7]. V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.

[8]. "Implementing Electronic Voting System With Blockchain Technology" Abhishek Kaudare, Milan Hazra. Anurag shelar, Manoj Sabnis. 2020 International Conference for Emerging Technology (INCET) Belgaum, India. Jun 5-7, 2020