*B*lock chain based E voting system

Charudatta Jadhav [a]
Vidya Kore [b]
Yayati Ghadge [c]
Dr. Aparna Pande [d]
Department of Computer Science and Engineering, Nutan college of Engineering and Research,Pune

Abstract

Voting is the foundation of the ultramodern republic. To ease the voting process, several electronic voting systems have been introduced, similar that the voting and counting processes can be fulfilled efficiently. The results would be the response to the public. Until now, still, an online electronic voting system has infrequently been enforced in practice due to the possibility of having the voting results tampered with through vote- apparel or cyber-attacks. Grounded on Block-chain technology, this paper proposes a protocol and system for electronic voting. The P2P network, the block-chain sub caste aims to produce a distributed database. It uses digital hand algorithms and encryption technologies to ensure data against tampering. It makes use of agreement algorithms to guarantee data thickness and applies timestamps to link data blocks end to end,icing chain structure preservation. And the operation of Ethereum completely integrates different functional modules as a whole and achieves agreement through evidence-of-work medium, miners mine, and the block-chain-posed network protocol is formulated to achieve coetaneous operation of the blockchain. Eventually, the smart contract stationed on Ethereum runs on an Ethereum-specific virtual machine and interacts with the underpinning blockchain through the Ethereum virtual machine.

This paper aims to estimate the operation of blockchain as a service to apply distributed electronic voting systems. And study blockchain-grounded voting and its styles. Doing so, it's determined how blockchain-grounded voting workshop, which types of advancing blockchain technology can be used, and what are the advantages and disadvantages of doing so. To ensure each namer is distinct, we use an Aadhaar Card for the unique identification of choosers.

Keywords: Blockchain, E-Voting, Security, Voters, Voting, Voting System

1 Introduction

Nowadays we have Democracy everywhere in the world so voting becomes very important for the future of a country or state. Voting has always been an important part of expressing one's views in popular society. From counting raised hands and filling out paper ballots to casting votes electronically, humanity is laboriously chancing ways to meliorate on a process that was formerly laborious, unreliable, and prone to crimes. Administering an electronic system for different types

of voting events, analogous to choices and general meetings, is perhaps the clearest- abbreviated way to annihilate or lessen the burden of counting votes manually and making misapprehensions in the process. Also in this system, there is a possibility of corruption or fake votes registration. For online voting systems, the critical security trouble of these prosecutions is their centralization. This means that they are controlled by a single main reality and have several security flaws, analogous to vulnerability to distributed denial-of-service (DDoS) attacks. A DDoS attack entails making the system inaccessible to the end-user by overfilling it with requests. also, given enough computing power, it might be possible to launch a state-position attack to anatomize and alter the voting data in all of the forenamed electronic voting systems. As a possible result of the downsides of traditional electronic voting, a system predicated on blockchain technology has been proposed Blockchain is a distributed ledger managed by a peer-to-peer agreement network, which allows its stored data to be transparent, empirical, and tamper-resistant by nature. The aforesaid benefits and a lack of central authority make it a potentially ideal platform for digital voting Still, as of writing this paper, there is no overview of the different processes for electronic voting on the blockchain. In light of that, this paper aims to address the main disquisition question of how blockchain technology can be used to enable electronic voting. Electronic voting machines can be tampered with during their manufacturing and in such cases, it does not even require any hacker or malware to manipulate the actual voting. There is a possibility that fraudulent votes can be done on EVM. Also nowadays verification of users or most of the work of election is paper-based which s a very tedious task and requires manpower also it's harmful to environment. So, the aim is to design a paperless digital fully distrusted, decentralized, and completely transparent voting system using Blockchain technology.
Motivation for this work is, Seen Election Process, It's a tedious task for booth managers who verify voters using paper. Also, Using an EVM machine there is the possibility of fraudulent votes. centralised structure designed for Election.To remove the fraud or fake votes, so blockchain can be used.It's impossible to change or modify data in blockchain.

2 Backbone

To Understand How Blockchain based Voting is Conducted, it is necessary to be familiar with some terms and methods related to blockchain voting. Smart contracts, SHA256, and ring signatures are important components of specific blockchain-based voting methods.

2.1 Blockchain

The blockchain was invented by Satoshi Nakamoto in 2008 as a public ledger for a cryptocurrency called Bitcoin. It is an ever-growing distributed ledger that consists of records that are linked using cryptography. These records are called blocks. Each block contains a timestamp, a cryptographic hash of the previous block, and data of the transaction As a characteristic of the blockchain, it is managed by multiple nodes in a peer to-peer network, each of which verifies the validity of a transaction before adding it to the blockchain. This kind of decentralization ensures that individuals cannot modify or add invalid blocks to the blockchain without reaching a majority consensus on the network. As such, a blockchain can be considered secure by design. Currently, there are three

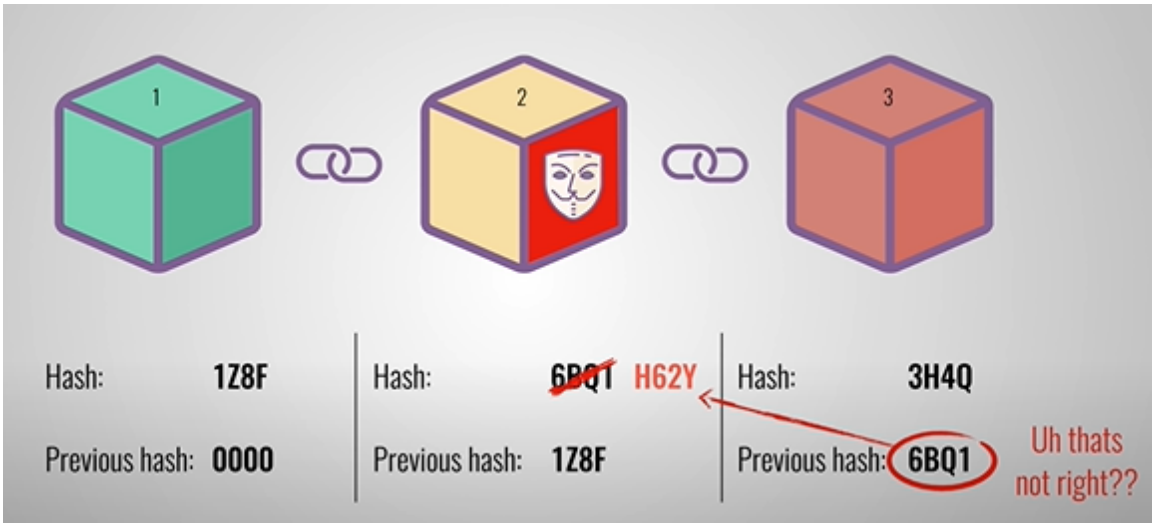

Figure 1: Architecture of Blockchain

main types of blockchain: public blockchain, private blockchain, and consortium blockchain. These blockchain types are characterized as follows: A public blockchain has no access restrictions. This means that anyone can read it, write to it by performing transactions, and even become a validator as one of the nodes. This type of blockchain is also called permissionless blockchain. Private blockchain has restrictions as to who can read and write to the chain, as well as validate it. It is generally controlled by an organization that aims to limit access to the blockchain internally. This type of blockchain can also be called a permissioned blockchain. A consortium blockchain is another type of permission blockchain. However, instead of being restricted to use by a single rganization, the ownership can be divided among several of them. The blockchain networks used in some of the voting processes in this paper include Bitcoin, Ethereum, and Hyperledger.

2.2 Smart Contract

Due to its decentralization and each node operating on a consensus algorithm, the blockchain is considered an immutable, secure data structure. Ethereum makes use of this property by expanding its blockchain with smart contracts A smart contract is a blockchain-based application that processes incoming information. Essentially, it is a script deployed on the blockchain that executes automatically as its functions are called. As such, it cannot be illegally removed or manipulated once written. This means that it can work transparently and autonomously without any external assistance. Many applications that would normally require a web server to function can be run through a smart contract instead.

2.3 Merkle Tree

Merkle tree is a fundamental part of blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use the Merkle Trees structure. Merkle Tree is also known as Hash Tree.

2.4 SHA-256

SHA-256 is a secure hash algorithm that was designed by the National Security Agency (NSA) in 2001 and used to secure communications on the federal level. It takes the input of plaintext in any size and encrypts it to a fixed-size 256-bit binary value. It is strictly a one-way function and cannot be decrypted without guessing the input data and running it through the SHA-256 algorithm to see if the hashed value is a match.

3 Literature Review

Earlier work done by various authors is summarised here.

- ”Decentralized Voting Platform on Ethereum Blockchain” : Building Voting systems with Ethereum Smart Contracts by the author named David Khoury, areas, the results of voting events have always been questionable and viewed Many existing E Voting systems are based

on centralized servers where voters must trust the planning authority with the integrity. In this paper we propose a new unconventional voting platform based include ensuring data integrity and transparency. As well as enforcing one vote platform, where clever, consistent and decisive contracts will be used by organizers, prior to the voting event to further voting rules. Their phone numbers without the need for an external company server.[Pun+21]

- " Blockchain-based e-voting recording system design": National elections still Problem with the traditional system is it fully controls the website and the system, potentially disrupting the database of many opportunities. the solution, because we accept a separate system and the entire database is Blockchain itself has been used in a Bitcoin system By adopting a blockchain in the distribution of information on electronic voting systems can reduce one of the most recordings of voting results using a blockchain. [HR17]

- "Web-based Open-Audit Voting": After Years of Research on the open web auditing They presented Helios, the first web-based, open-source survey on The voting system. And its Protocol Helios are publicly accessible today: anyone can create and run an election, and any interested viewer can research the whole process. Helios is ideal for online software communities, local clubs, student government, and other areas where honest, confidential elections are required but enforcement is not a serious matter. It works by Encrypting and Shuffling the Audits Covered by Ben Adida in the Research. [Adi08]

- In the Scantegrity ballot, each candidate has a random Letter Paired with the Position. It is a voting system that offers independent verification without changing voter marks on optical scan ballots. It complies with unencrypted paper audit records. It is recorded by David Chaum and Aleks Essex, Richard Carback, and Jeremy Clark in the Research Process. [Cha+08]

- In "Multi-objective Optimization of Block Size Based on CPU Power and Network Bandwidth for Blockchain Applications" the Authors Nikita Singh and Manu proposed a system that solves the Block size optimization issue on the In the proposed approach, multi-objective optimization is made, and 40 different solutions are available based on transaction selection time and block build time. The choice of a particular block size as the optimal solution is based solely on the CPU processing capacity, output and available network bandwidth and delays, where the application will be used. [SV21] [Kha+12] [FOO93] [Jon03] [Sad+20]

4 Proposed System Methodology

our proposed system works as follows

4.1 System Architecture

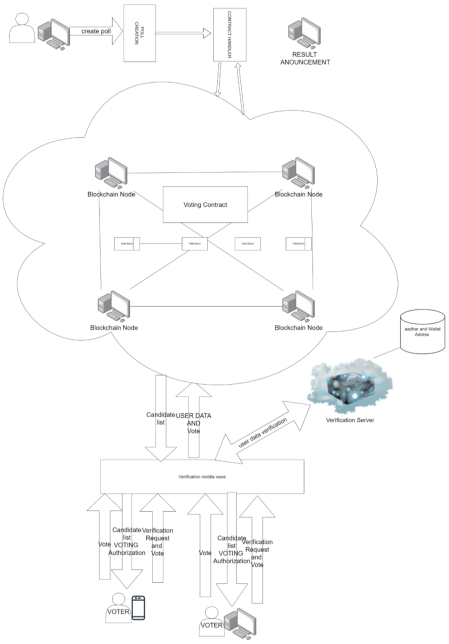

Figure 2: System Architecture Of Voting System

The Contract manager or admin Initiates the Poll and Control Each and every action and flow in the process. He can Add Booth Managers and assign their areas to work. They are the ones who will Monitor and Verify the Actual voters who will cast their votes. Performed on Web App.After verification Voter is redirected to the voting page where they can vote irrespective of the device used the can vote anywhere. Verification is done with the data from a central server and the Aadhaar Id of the voter compared and checked if it is valid then the process is initiated forward.Votes are stored on both the system first is the central server and the second on the Ethereum blockchain. Thus, the data store is immutable and publicly accessible so any changes which are false-positive can easily be identified.

4.2 System Model

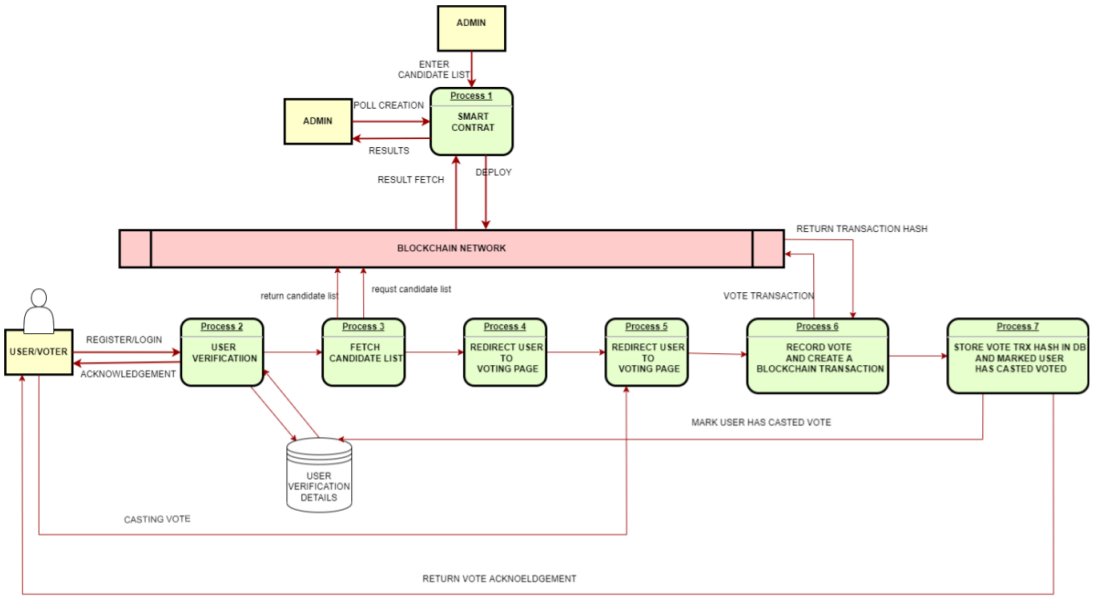

Figure 3: Block Diagram Of Voting System

1. Initial Setup : Admin will Add important things from his account like Entering Candidate List according to Constituencies into System, constituencies, booth manager's details. Then Admin will Initialise the Poll or event for an election.

2. Voting: booth manager will be able to log in after adding by the admin. Verification of voters will be done via booth manager using Aadhaar Card and OTP. Check If the Voter is Present and Has not Voted or not. upon the validation, it will be redirected to Voting Page,then voter will Cast A vote.

3. Storing Vote : Votes of Voter will be stored in database and blockchain platform and it will now not be able to modify also voters can't do vote more than once. calculation part will also be done in this step only.

4. Results : Fetch the results from database and Blockchain Cross verifies them and after that declare the result which candidate have won the election.

4.3 Flowchart

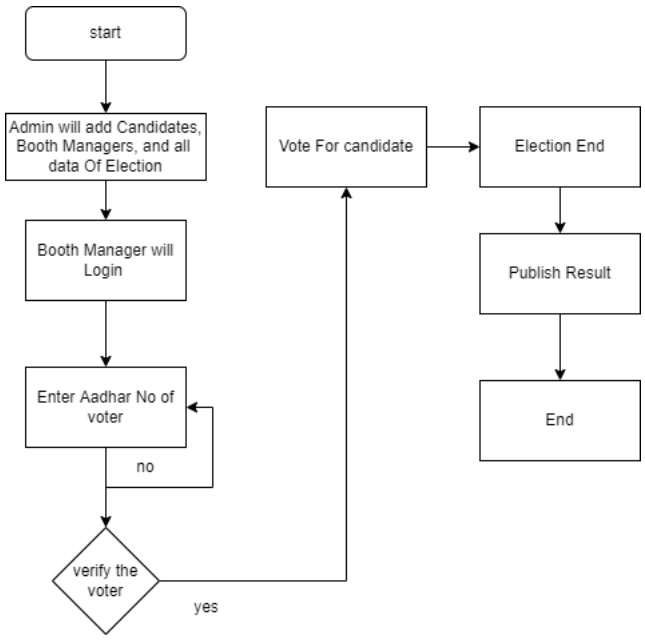

Figure 4: Work Flow Diagram

The figure shows the actual flow of the voting system. The flow begins with input image taken as input.

4.4 Pseudo code of The Algorithms

The Algorithms used for this system is Proof of Stake.

```
pragma solidity >=0.6.0 <0.9.0;
contract vote{ //create map
    mapping(uint256=>bool ) public CandidateIdtoBool;
    //CandidateIdtoBool[_candidateId] = true;
    mapping(uint256=>string ) public CandidateIdtoName;
    mapping(uint256=> uint256) public partyIdToCandidateId;
   mapping(uint256=> uint256) public
    candidateIdToVotes;
    //name will be stored in memory
```

```
function addCandidate(string memory _candidateName,
uint256 _candidateId, uint256  _partyId) public
{  if (validCandidate(_candidateId) )
    { revert("Not a valid canditate ");}
    else
    { CandidateIdtoName[_candidateId] = _candidateName;
    CandidateIdtoBool[_candidateId] = true;
    partyIdToCandidateId[_partyId] = _candidateId;
    }  }
//checking if candidate is valid
function validCandidate(uint256 _candidateId) public view returns(bool)
{ if(CandidateIdtoBool[_candidateId])
        {  return true; }   else{ return false;   }     }
// voting for a candidate
function voteForCandidate(uint256 candidateId) public
{    if (validCandidate(candidateId) )
    {   candidateIdToVotes[candidateId] += 1;   }
    else{  revert("Not a valid canditate ");   }      }
function getVotes (uint256 candidateId)
public view returns(uint256)
{    if (validCandidate(candidateId) )
    { return candidateIdToVotes[candidateId];
    }  else{ revert("Not a valid canditate ");   }   }
function removeCandidate(uint256 candidateId)
public
{        if (validCandidate(candidateId) )
   {     delete candidateIdToVotes[candidateId];
    delete CandidateIdtoName[candidateId];
    delete CandidateIdtoBool[candidateId];
    delete partyIdToCandidateId[candidateId];
    }         else{ revert("Not a valid canditate ");
```

```
}     } }
```

4.5 Advancement System

Authentication Middleware: It provide a authentication layer through which a voter's data is verified and is further taken to vote. Middlerware is based on Django a python web development framework which is highly scalable and flexible. Modular Approach : Django is MVT Framework which helps to add new functions to web app as modules and remove or update existing modules thus it becomes fully modular. Area wise Candidate and Voter arrangement : Database is designed according to the parliamentary structure of Indian voting system. Identification of False Votes : Middleware helps in some degree to identify false votes and prevent such voters from voting further enhancements can be made to it for using bio-metric verification of voters.Well Fitted Architecture for Indian Electoral System : System can be easliy adopted in the Indian electoral system which can reduce costs of today's election system.Any change In central Database can be found and tracked as votes are stored on blockchain : For Storing the votes Blockchain is used so the once recorded votes cannot be manipulated and it becomes difficult to tamper with the recorded data.

5 Results

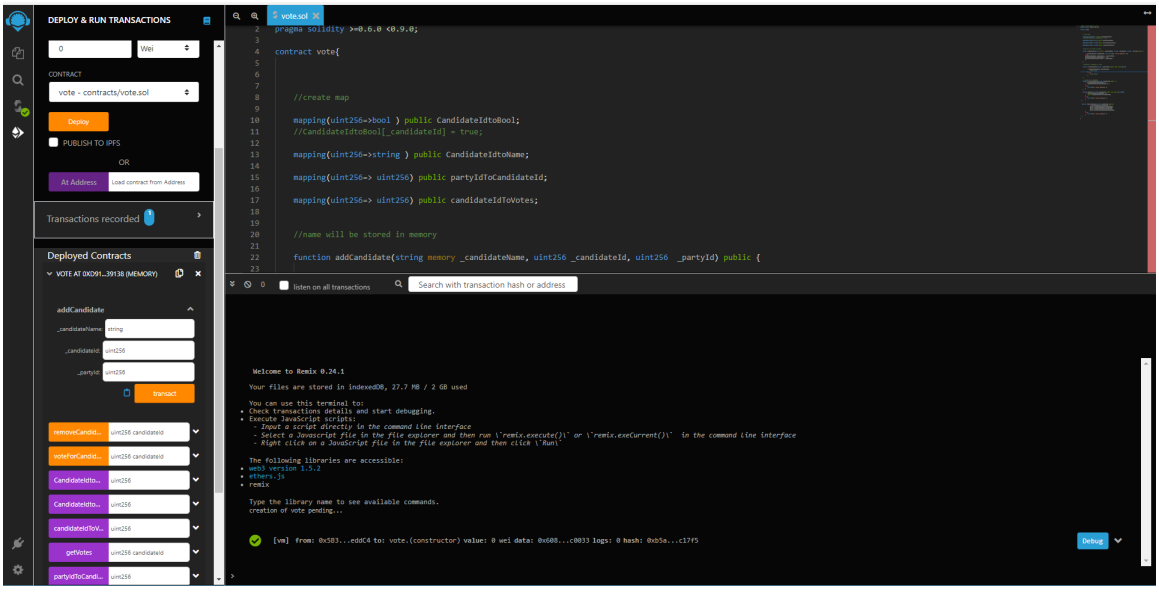

Figure 5: Blockchain Smart Contract add candidate

In This image Remix IDE is shown which used for writing smart contracts and compile them.On the right hand side there is a toolbar which has multiple options which are **File explorer, Compiler, Deploy and Transact**.There is a number of options to select from for deployment of contract in Deploy and Transact Option.In Compiler Option you can select compiler version for compiling your smart contract.

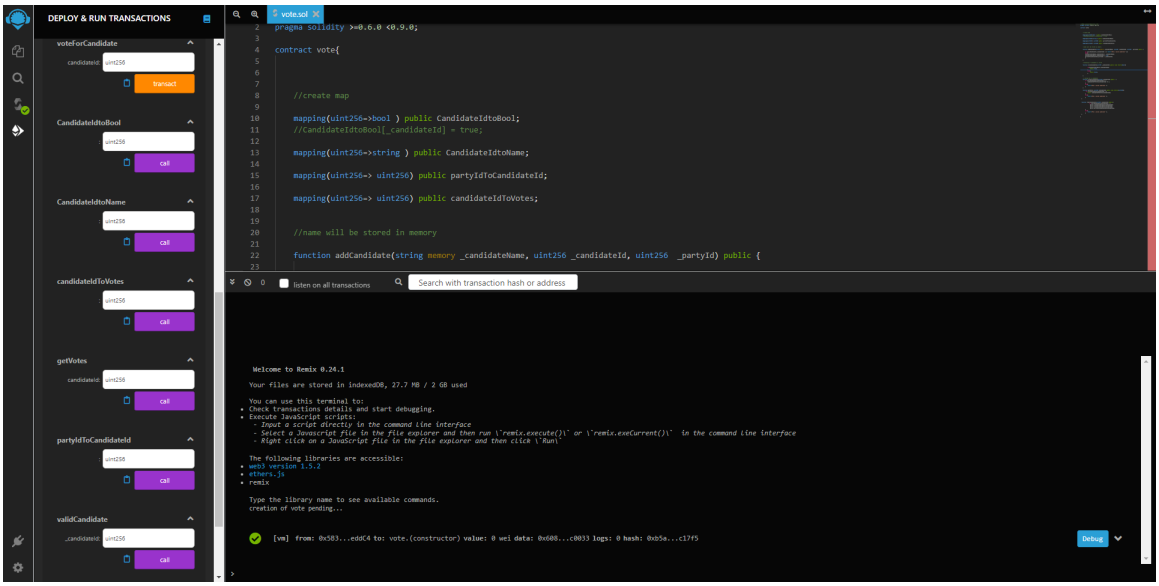

Figure 6: Blockchain Smart Contract other methods

On the right side A text field and A button associated to it.The text filed above the orange button is block chain transaction,the button in the purple denotes a call.

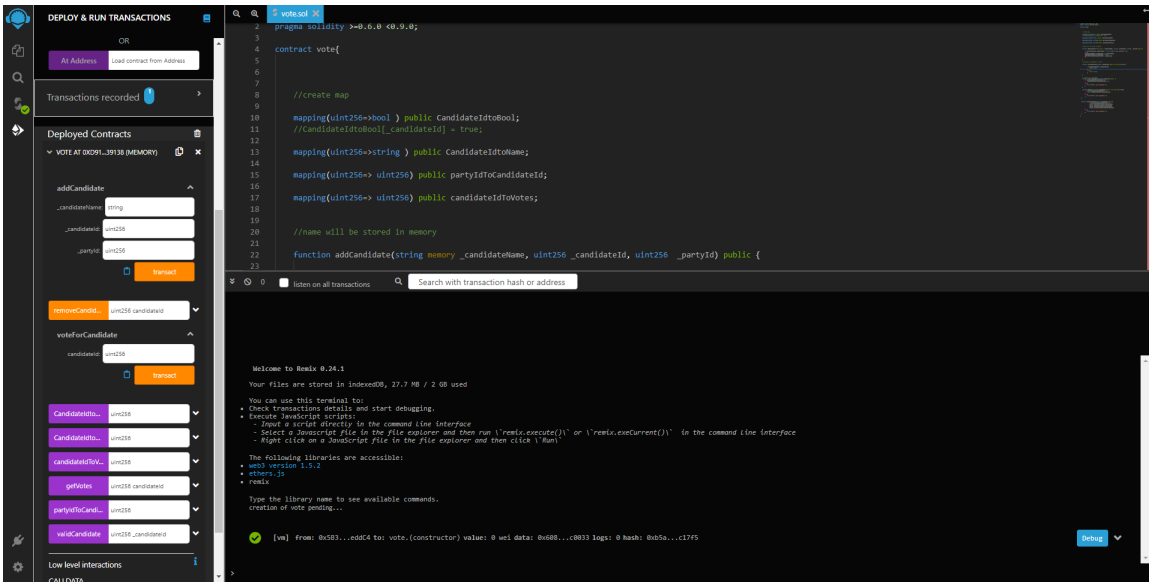

Figure 7: Voting Candidate on smart contract

This Image shows transaction which is used to add voters on the contract block. When you Click on the orange button the transaction is initiated.

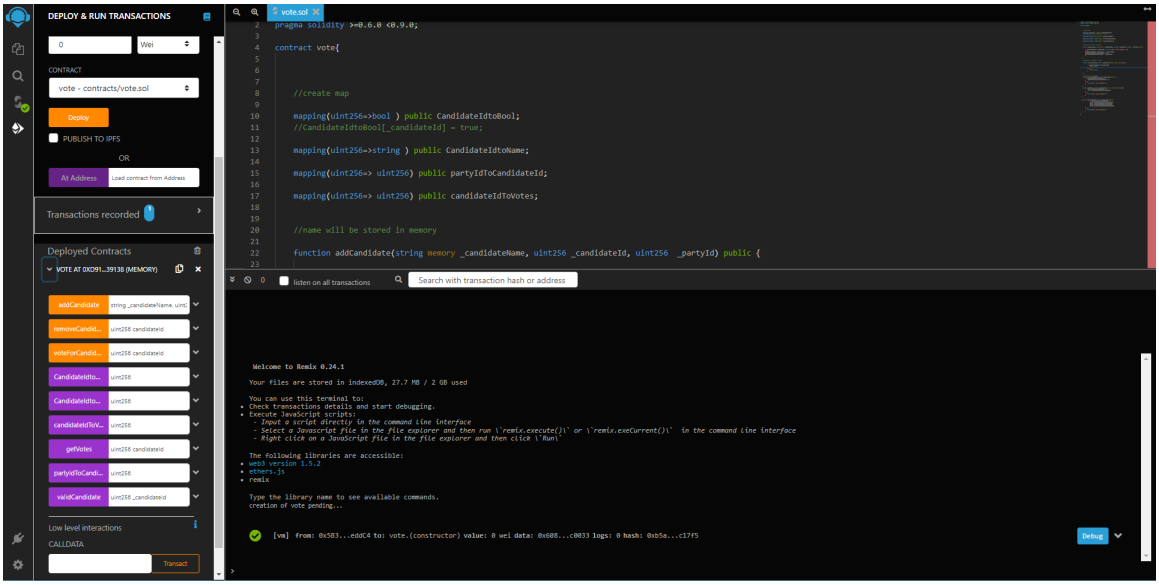

Figure 8: Deployment of Contract

This Image shows deployment contract on Eethereum

6 Conclusion

This e-voting is more open, transparent and independently auditable.Removes any threat to link votes for certain parties back to individual voters.Maintaining the ability to track who has voted and how many votes are present. Our research allowed us to show blockchain technology can be used to enable secure electronic voting.Blockchain voting can be used for both polls and elections of various scales. Four main methods were identified to provide a general overview of a blockchain-based voting process.Smart contracts,Custom blockchain, Cryptographic signatures.The advantages and limitations of blockchain voting were also determined. As a result of the literature review, A Review was created providing an overview along with references for different blockchain-based solutions.

References

[FOO93] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. "A practical secret voting scheme for large scale elections". In: *Advances in Cryptology — AUSCRYPT '92*. Ed. by Jennifer Seberry and Yuliang Zheng. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 244–251. ISBN: 978-3-540-47976-5.

[Jon03] Douglas W. Jones. "The Evaluation of Voting Technology". In: *Secure Electronic Voting*. Ed. by Dimitris A. Gritzalis. Boston, MA: Springer US, 2003, pp. 3–16. ISBN: 978-1-4615-0239-5. DOI: 10.1007/978-1-4615-0239-5_1. URL: https://doi.org/10.1007/978-1-4615-0239-5_1.

[Adi08] Ben Adida. "Helios: Web-based Open-Audit Voting". In: *17th USENIX Security Symposium (USENIX Security 08)*. San Jose, CA: USENIX Association, July 2008. URL: https://www.usenix.org/conference/17th-usenix-security-symposium/helios-web-based-open-audit-voting.

[Cha+08] David Chaum et al. "Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting". In: *Security Privacy, IEEE* 6 (June 2008), pp. 40–46. DOI: 10.1109/MSP.2008.70.

[Kha+12] Dalia Khader et al. "A Fair and Robust Voting System by Broadcast". In: *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)* 205 (Jan. 2012).

[HR17] Rifa Hanifatunnisa and Budi Rahardjo. “Blockchain based e-voting recording system design”. In: *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. 2017, pp. 1–6. DOI: 10.1109/TSSA.2017.8272896.

[Sad+20] Kazi Sadia et al. “Blockchain-Based Secure E-Voting with the Assistance of Smart Contract”. In: June 2020, p. 161. ISBN: 978-981-15-4542-9. DOI: 10.1007/978-981-15-4542-9_14.

[Pun+21] Puneet et al. “Decentralized Voting Platform based on Ethereum Blockchain”. In: *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*. 2021, pp. 1–4. DOI: 10.1109/ICAECT49130.2021.9392580.

[SV21] Nikita Singh and Manu Vardhan. “Multi-objective Optimization of Block Size Based on CPU Power and Network Bandwidth for Blockchain Applications”. In: Jan. 2021, pp. 69–78. ISBN: 978-981-15-5545-9. DOI: 10.1007/978-981-15-5546-6_6.