International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

A Decentralized Voting Application using Blockchain Technology

Manoj Shrinivas[1], Chandan S[2], Mohammed Shamail Farhan[3], Ramyashree K[4]

[1,2,3,4]*Eight Semester, Dept. of Ise, The National Institute of Engineering, Mysore*

Abstract - *In centralized systems, the results of voting events have always been questionable and not trustworthy by voters. Most existing E-Voting systems are based on centralized servers where the voters must trust the centralised organizing authority for the integrity of the results. In this paper we have proposed a decentralized voting platform based on Ethereum Blockchain. This idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Distributed Systems is an exciting technological improvement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. Here we evaluate the application of blockchain as service to implement distributed electronic voting systems. We evaluate some of the popular blockchain frameworks that offer blockchain as a service. We then propose an electronic voting system based on blockchain that addresses all limitations we discovered. The main features of this system include ensuring data integrity and transparency, and enforcing one vote for every poll with ensured privacy, security and decreases the cost of hosting a nationwide election. To accomplish this, the Ethereum Virtual Machine (EVM) is used as the Blockchain runtime environment, on which transparent, consistent and deterministic smart contracts will be deployed by organizers for each voting event to run the voting rules.*

***Key Words*: Blockchain, Ethereum, Smart Contracts, IPFS, Metamask, Adding candidate, Voting, Html, Css, Javascript.**

1. INTRODUCTION

Voting has always been regarded as the primary method used by individuals to share their opinions on controversial issues and debates. It is a democratic practice, enabling people to formally express their choice against a ballot question, candidate election, political party and others [1]. In every democracy, the security of an election is a matter of national security.

With the goal of minimizing the cost of having a national election, while and increasing the security of an election, the computer system has been trying to make electronic voting system more secure [2] [3].

From the dawn of democratically electing candidates, the voting system has been based on pen and paper. The traditional pen and paper election system which fails to provide the voting process traceable and verifiable is replaced by the new election system. Electronic voting system has been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine or server can hack or alter the votes, thereby affecting all votes cast on the machine.

Blockchain technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database. The blockchain technology is therefore considered by many, including us, to be the ideal tool, to be used to create the new modern democratic voting process. Blockchain is gaining attention in several domains, even in the telecommunication industry [5]. Here we evaluate the use of blockchain as a service to implement an electronic voting (e-voting) system by following original contributions such as research existing blockchain frameworks suited for constructing blockchain based e-voting system, and propose a blockchain-based electronic voting system that enable liquid democracy.

The main contributions of Blockchain are Enforcing voting data immutability and data integrity ensuring robustness and reliability of the voting system, Decentralizing the registration and validation mechanisms of voters, Transparency, clarity and determinism of the voting environment, Public visualization of the smart contracts votes, Restricting each voter to have a single vote per valid and Privacy-aware regarding the confidentiality of the recorded votes.

2. EXISTING SYSTEM

In today's world, widespread mistrust towards the government and interference in countries processes by external actors have made the democratic process of voting more critical than ever. People have had their human rights violated and their fundamental freedoms provided by their constitution taken away. In such an atmosphere, having a fair and transparent election is something that is paramount for the freedom most people enjoy today. The pitfalls of the current system of ballot voting are being taken advantage of by people or organizations looking to gain power. The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an Election commission or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral scams such as voter fraud, ballot stuffing and booth capturing. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization.

3. BACKGROUND ON BLOCKCHAIN TECHNOLOGY AND ETHEREUM

To solve the problem, we use Blockchain technology which is decentralised, distributed, immutable, irreversibility, distribution of joint accounting, asymmetric encryption and provides data-security. This new technology works through four main features:

a) The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

b) There is distributed control over who can append new transactions to the ledger.

C) Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

d) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

These technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database.

Blockchain can be referred to as a public decentralized database with replicates distributed over several nodes simultaneously [6]. In Blockchain there is no authority in charge of managing and maintaining the ledger of transactions. The validity of the ledger's version is established through a consensus mechanism among the validating nodes. The use of Blockchain technology allows a secure validation of transaction's data integrity. Bitcoin, for instance, is the first application developed over Blockchain by Satoshi Nakamoto [7]. On another hand, Ethereum Blockchain [4] is an open-source, distributed and decentralized computing infrastructure that executes programs called smart contracts. It is developed to enable decentralization for applications and not only for a digital currency. It is achieved using a virtual machine (Ethereum Virtual Machine, EVM) to execute a complete scripting language. Unlike Bitcoin in which only Boolean evaluation of spending conditions are considered, EVM is somehow similar to a general-purpose computer that simulates what a Turing machine can execute. Changing the state of a contract in the Blockchain requires transaction fees which are priced in Ether. Ether is considered as the fuel for operating the distributed application platform.

3.1 ACCOUNT TYPES IN ETHEREUM

There are two types of accounts in Ethereum:

1) Externally Owned Accounts (EOA): An account identified by a wallet address and controlled by a private key. The holder of this private key can transfer ether and sign transactions from this account. Externally Owned Accounts are considered user type accounts and are linked to unique cryptographic keys pair, generated upon account creation. The public key is used to reference the account and also called EOA address whereas the private key on the other hand is used to sign transaction before executing any type of transaction on the network to prove authenticity. EOAs have balances which hold Ether cryptocurrency [8].

2) Smart Contract: A smart contract is an account that is controlled by its own code [9]. It is considered as an autonomous agent executed by the EVM and is the core foundation and the main building blocks of any Decentralised Application [10] . Once this code is deployed on the Blockchain, the EVM will take care of running it as long as the conditions apply. It is important to note that smart contracts once deployed to the Blockchain network, they can be visited and viewed via their address with all their associated transactions (to address, from address, timestamp, etc...). Triggering functions in the smart contract can be performed from any account as long as the following two conditions are met:

a) Address of the smart contract is known.

b) The function caller has sufficient Ether to trigger.

Smart Contracts provide an important added value: The code ruling the business logic is now public (easily verifiable) and not obscure as in conventional servers.

3.2 PRIVATE ETHEREUM BLOCKCHAIN

Not only public Blockchain is available, but also a permissioned version exist. This version is also referred to as Private Blockchain [13]. The question whether to adopt each type depends heavily on the application's requirements. In a public Blockchain, any EOA can send transactions to other addresses and explore the network using online explorers such as Etherscan. In a permissioned Blockchain, a central authority is needed to control and maintain its own ledger. In a country election process for instance, a permissioned Blockchain is preferred as the government is in control of the election process.

4. LITERATURE REVIEW AND RELATED WORK

We present in this section various solutions that attempt to integrate E-voting and Blockchain to enable decentralization of voting services. We then highlight the added value of our proposed system compared to the others.

a) Towards Secure E-Voting Using Ethereum Blockchain: Ali Kaan Ko et al. discuss in their paper entitled "Towards Secure E-Voting Using Ethereum Blockchain" [14] a decentralized voting solution based on Ethereum Blockchain. It states that an E-Voting system must be secure by being fully transparent (privacy-aware) and not allowing

duplicated votes. It suggests deploying the E-Voting application as a smart contract and allowing users with valid EOAs to vote on that contract (once per address to a single question). Nevertheless, this solution lacks true automated address verification protocol since the EOAs get their right to vote from a Centralized Authority to become eligible voters. The main advantages it offers are business rules transparency and single vote restriction per EOA. 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)

b) The Future of E-Voting: In their paper entitled "The Future of E-Voting", Tarasov et. al discussed E-Voting and its potential use with Blockchain [15]. In addition to transparency, privacy, and integrity which became inherent properties of Blockchain Decentralized Applications, this solution proposes a registration phase to verify the users' identities. Registration is the first step of the protocol, and is required as part of the identity verification for audit purposes. It helps keeping track of which voters have cast a ballot. Although the verification process is done using a Challenge-Response handshake protocol, it involves again a server (Centralized Authority) to handle the verification process and add the users' data (email addresses) to the database. It is worth mentioning that email addresses are relatively easy to spoof nowadays.

c) Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain: Fernando Lobato Meeser, in his paper entitled "Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain"[16] discusses two types of ongoing issues with E-Voting solutions. First, the capability of anyone to tally the results from the smart contract before having all the votes casted, and second, the anonymity of the votes since public keys can be associated with the recorded votes. In this paper, the author presents the implementation of a voting system as a smart contract running on Ethereum that uses threshold keys and linkable ring signatures. Nevertheless, this solution again includes a registration phase, and voters rely on a Centralized Authority to register their public key for casting a vote.

d) "Removing Trusted Tallying Authorities Self- Enforcing E-Voting over Ethereum": Published paper by Patrick McCorry et at.[17], claim that while preserving the voters privacy, their protocols allow anyone, including observers, to verify the integrity of the election without having to trust authorities. They achieve by namely Open Vote Network (OV-net), Direct Recording Electronic with integrity (DRE-i), and DRE-i with enhanced privacy (DREip). In spite of that, their system requires an authority to setup a list of eligible voters and transfer them to the Ethereum Blockchain before the elections starts. Although having a predefined list of voters is a good choice for certain use cases, but the challenge remains in fully decentralizing the voting process.

5. PROPOSED SYSTEM

In this section we introduce our proposed voting system that aims at solving the existing barriers.

5.1 SYSTEM COMPONENTS

The proposed platform consists of the following components:

1) Web application: The web application allows the voters and the Administrator to Authenticate for the further process. The administrator adds the candidate list and then initiate an HTTP request to the Event Management Server containing the entered data. The goal of this Web application is to be available as an Application Programming Interface [23] allowing administrator to add the candidates list and allow the selected votes to vote (by authentication through database). As the voting process takes place in the Ethereum network, it is mandatory to have an interface connecting the web application to the Blockchain network. Therefore, an Ethereum light client and Metamask application is integrated within the web application. All transactions transmitted from the web application are sent to the Blockchain network through this client.

2) Event Management Server: The main goal of the Event Management Server is to deploy the Smart Contract to the network with the data (questions and answers) received from the web application. Therefore, it contains an Ethereum Wallet (address) which is required to deploy the contract, a full node to interface the Ethereum network, and a database to store the list of contract addresses which will be fetched later by the web application.

3) Smart contracts: Two types of smart contracts exist in our system: a) Election contract, b) Voting contract. The Election contract serves the adding the candidates and initiate the voting by restricting one user vote only once. The voting contract authenticates the voters and initiates the voting process and increments the count of the vote when voted and returns the total votes. Appendices A and B list the code of both contracts.

4)IPFS: It plays an important role in hosting the decentralised web application online by which voters can vote through internet from any part of the world.

5)Metamask: It is an extension for accessing Ethereum enabled distributed applications, or "Dapps" in your browser. The extension injects the Ethereum web3 API into every website's javascript context, so that dapps can read from the blockchain .MetaMask also lets the user create and manage their own identities via private keys, so when a Dapp wants to perform a transaction and write to the blockchain, the user gets a secure interface to review the transaction, before approving or rejecting it.

5.2 ADDING THE CANDIDATES

The Administrator uses the web application discussed previously to create a new voting event by adding the candidates and can see the results realtime. The Administrator is requested to add the candidate through the web. Technically, creating a voting event means creating a voting contract on the Blockchain. Therefore this transaction must be charged for the administrator as transactions cost in Ethereum. After securing the transaction cost, the web app deploys the contract to Ethereum the network. The address of the newly created smart contract will be returned to the administrator.

5.3 VOTING

While Voting is initiated, the application calls the VoteForCandidate(string option) method of the designated smart contract deployed on the EVM. Next, the voting contract contacts the election contract to check if the user is already existed. Then, it checks if the user already voted or the event is finished. If the conditions are satisfied, the contract increments the count of the selected option, marks the user as voted, and takes it to the end page.

The contract automatically rejects duplicate votes, allowing to restrict one vote per user. This is considered the major advantage of our system compared to the others.

6. IMPLEMENTATION AND RESULTS

To validate the proposed system, we implemented the solution using various technologies. Solidity, a contract oriented programming language for writing voting smart contracts [19], NodeJS [20]: Server side scripting for the Event Management Server, Web3js to interface the light client [19], and Html, Css for the frontend user interface, Javascript for the backend interface, Database for user authentication for voting. The Ropsten Testnet [22] is used to simulate the Blockchain network. Metamask for initiating the transactions. Ipfs for hosting the decentralized website online.

Fig. 1. The Home page of the web application

Fig. 2. Administrator login page

Fig. 3. Voter login page

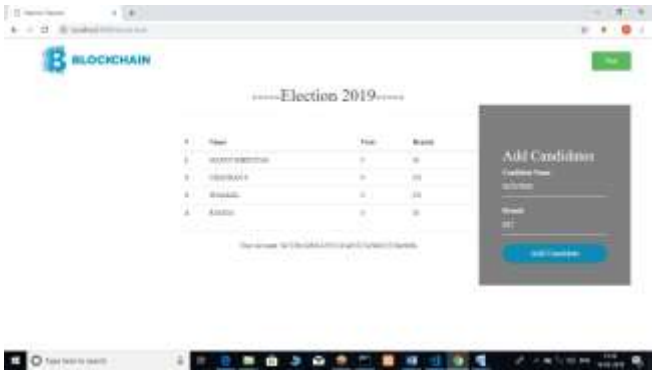


Fig. 4. Administrator adding the candidates

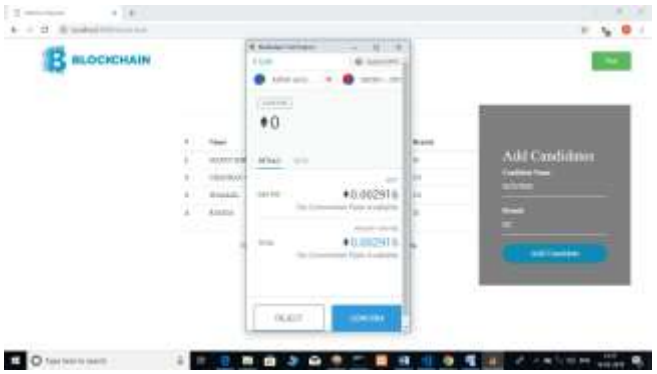


Fig. 5. Administrator initiating the transaction to add candidates using Metamask

Fig. 6. Voting Page where voter can vote for the candidate listed

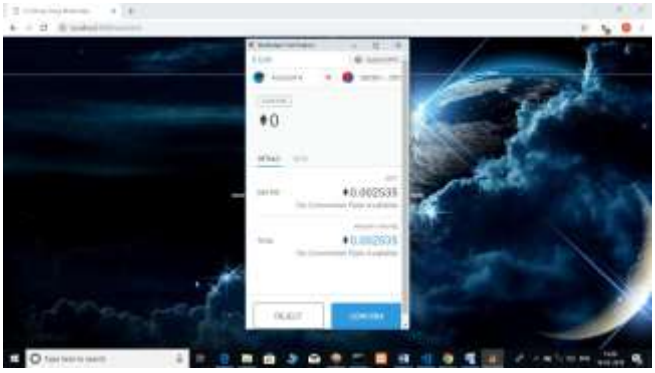


Fig. 7. Voter initiating the voting transaction using Metamask

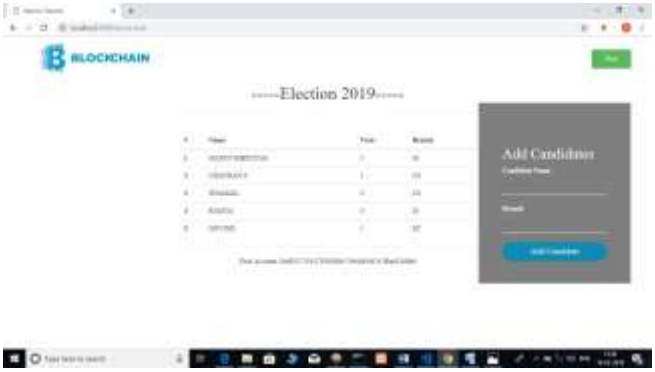


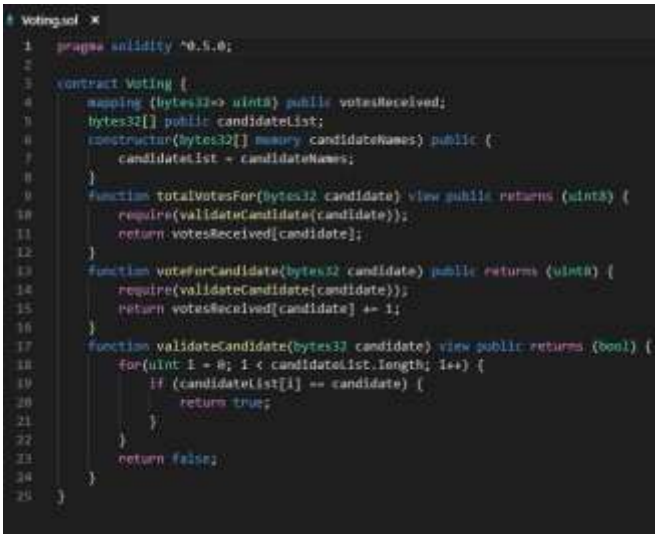
Fig. 8. Administrator page where the results are viewed

APPENDIX A

ELECTION CONTRACT

APPENDIX B

VOTING CONTRACT



```
Voting.sol
pragma solidity ^0.5.0;

contract Voting {
    mapping (bytes32=> uint8) public votesReceived;
    bytes32[] public candidateList;
    constructor(bytes32[] memory candidateNames) public {
        candidateList = candidateNames;
    }
    function totalVotesFor(bytes32 candidate) view public returns (uint8) {
        require(validateCandidate(candidate));
        return votesReceived[candidate];
    }
    function voteForCandidate(bytes32 candidate) public returns (uint8) {
        require(validateCandidate(candidate));
        return votesReceived[candidate] += 1;
    }
    function validateCandidate(bytes32 candidate) view public returns (bool) {
        for(uint i = 0; i < candidateList.length; i++) {
            if (candidateList[i] == candidate) {
                return true;
            }
        }
        return false;
    }
}
```

7. CONCLUSIONS AND FUTURE WORK

In this paper we have proposed a decentralized voting platform based on Ethereum Blockchain. This idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. It also opens the door for a more direct form of democracy, allowing voters to vote from any part of the world through internet and can monitor that their vote has been counted. Blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency and guarantee that each individual voters vote is counted from

the correct district, which could potentially increase voter turnout.

This system could be developed further to make it more eligible for national government elections, based on fingerprint authentication, using Artificial intelligence for facial and single user authentication and by using upcoming technologies for the easy, better and secured voting.

REFERENCES

[1] A. J. Bott, Handbook of United States election laws and practices: political rights. Greenwood Publishing Group, 1990.

[2] W. R. Mebane Jr, "Fraud in the 2009 presidential election in iran?" Chance, vol. 23, no. 1, pp. 6–15, 2010.

[3] R. Jim´enez and M. Hidalgo, "Forensic analysis of venezuelan elections during the ch´avez presidency," PloS one, vol. 9, no. 6, p. e100884, 2014.

[4] V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, 2014.

[5] E. F. Kfoury and D. J. Khoury, "Secure end-to-end volte based on ethereum blockchain," in 2018 41st International Conference on Telecommunications and Signal Processing (TSP). IEEE, 2018, pp. 1–5.

[6] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[9] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 79–94.

[10] M. Pilkington, "11 blockchain technology: principles and applications," Research handbook on digital transformations, p. 225, 2016.

[11] Ethereum, "Light ethereum subprotocol." [Online]. Available:https://github.com/ethereum/wiki/wiki/Light-client-protocol .

[12] R. C. Merkle, "Method of providing digital signatures," Jan. 5 1982, uS Patent 4,309,569.

[13] M. Vukoli´c, "Rethinking permissioned blockchains," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017, pp. 3–7.

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

[15] P. Tarasov and H. Tewari, "The future of e-voting." IADIS International Journal on Computer Science & Information Systems, vol. 12, no. 2, 2017.

[16] F. L. Meeser, "Decentralized, transparent, trustless voting on the ethereum blockchain," 2017.

[17] P. McCorry, E. Toreini, and M. Mehrnezhad, "Removing trusted tallying authorities," Technical report, Newcastle University, 2016. Cited on, Tech. Rep., 2016.

[18] E. F. Kfoury and D. J. Khoury, "Secure end-to-end voip system based on ethereum blockchain," Journal of Communications, vol. 13, no. 8, pp. 450–455, 2018.

[19] C. Dannen, Introducing Ethereum and Solidity. Springer, 2017.

[20] J. Wilson, Node. js 8 the Right Way: Practical, Server-side Javascript that Scales. Pragmatic Bookshelf, 2018.

[21] R. K. Camden, Apache Cordova in action. Manning Publications Co., 2015.

[22] K. Iyer and C. Dannen, "The ethereum development environment," in Building Games with Ethereum Smart Contracts. Springer, 2018, pp. 19–36.

[23] D.Orenstein, "Quickstudy: Application programming interface (api)," 2000.