iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XII **Month of publication:** December 2019

DOI: http://doi.org/10.22214/ijraset.2019.12167

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Secure E-Voting System using Blockchain Technology

Komal Agrawal[1], Shivani Gupta[2], Reetika R. Baberwal[3], Mukta Dhiman[4]
[1, 2, 3]MCA Student, [4]Assistant Professor, Dept. of Computer Applications, NIT Kurukshetra, India

Abstract: ***With the advent of IoT, gadgets are now becoming more smart and independent. Truth is that the transformation towards the innovation is in progress yet there are still flaws, mainly in security areas like dependence on the data. Keeping in mind the advancement of IoT in the future, trusting in this vast approaching data source is of great importance. Blockchain is reached up to the position where it became the key innovation that will change the way we share data. Providing trust in conveyed situations, without using any advanced technical team is a development, which could change the way of working of numerous enterprises, the IoT amongst them.***

We can say with confidence that the concept of Blockchain, which is the technology behind crypto currency [3] Bitcoin [1], introduced a new era in the world of Internet and online services. In this paper, we will talk about develop a secure E-voting system using Blockchain technology where nobody can manipulate the votes and every user can vote only once. This is possible using the advantage of Ethereum smart contracts [2]. Smart contracts make it a powerful tool for the digitization of services in the Ethereum platform.

Blockchain with smart contracts develops a safe, cheap, secure and transparent E-voting system. Ethereum and its network are suitable for it. Due to its consistency, large scale use and provision of smart contract logic. E-voting is an application that is possible using Blockchain technology with infused smart contracts. It needs to be digitalized over the Internet & that's what we will be working upon.

Keywords: Blockchain, Ethereum, Smart Contract, Bitcoin, EVM.

I. INTRODUCTION

Blockchain technology come into view after the widespread acceptance of Bitcoin[1]. At the starting, blockchain was used only as a money transfer and trade, but further study suggested its use over other areas because of its transparency in the system. Not only money transfer but other structured information can be stored in the distributed chain using some cryptic methods. The software programs enforced by smart contracts [2] can be written in blockchain and are immutable. Once written they can't be manipulated. Hence, they are transparent and are available over the Internet forever.

A. Blockchain, as the name specified is a chain of blocks and each block contains data. It is basically a decentralized, distributed database or a ledger.

B. Decentralized, because nodes on the network doesn't depend on the third party. Every node have all the data. If any node fails down then it would not affect the other nodes on the network.

C. Distributed, Blockchain is distributed in the sense that all the nodes on the network are connected to each other. So every node on the network can communicate with other nodes directly.

D. Database, Blockchain is the database as it is used to store data in blocks. We can read, write or append the data from the blocks.

E. Ledger, it's called ledger because as on ledger we can't change the previous transaction or data. Same as, on the blockchain we can't modify the previous data but we can add more data. So nobody can change the votes or code.

F. Because of these features of the blockchain, and ability to don't change the previous data, blockchain solutions are transparent, highly trustworthy and incorruptible.

G. Ethereum is becoming rising start in the world of cryptocurrency. Ethereum is an open programming stage dependent on blockchain innovation that empowers engineers to construct and send decentralized applications. It gives us the functionality of Smart contracts. Ethereum is distributed public blockchain network like the bitcoin. In spite of the fact that there are some noteworthy specialized contrasts between the two, the most significant qualification to note is that Bitcoin and Ethereum vary generously in reason and capacity. Bitcoin is mainly used for electronic money transfer while Ethereum blockchain centers on running the programming code of any decentralized application.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

II. LITERATURE REVIEW

For the better understanding of the key concepts and technology used for the development of blockchain, the ethereum white paper [4] was being used as an initial reference. It consist bitcoin's concepts such as how it was invented, how it is a state transition system, mining concept, how it can be used as an alternative, smart contracts for scripting and it also gives information about the technology used by ethereum for developing blockchain based application, ethereum accounts, messages and transactions.

E-voting system is a technology which is being considered by few nations. Estonia [5] is one such country which is a successfully implementing E-voting system since 2005 and is the first nation to use online voting. Since then many associations used lawfully restricted online framework, for eg, the Austrian federation of students, Switzerland[6], the Netherlands, Norway etc. even though a large amount of work is done in this area still some security issues and still the online voting system is not generally used over conventional voting system around the world.

Followmyvote[7], is a start-up in which anonymous voters vote and the counting is done. Some technical formulas are used by the applications to distinguish between valid and invalid voters. This application has future scope but is going to take time before it comes into play.

In [8], the work has been done by using two blockchains, one is used for maintaining the information about votes and other for information about voters. Different voting levels are introduced in the system

making it a complex architecture. Like, municipality level, another is at central level. This causes congestion in the network and is unreliable making it difficult to real implementation.

During discussion over the paper by Ali Kaanko Et Al[9] a decentralized voting application solution based on Ethereum blockchain came into play. It says that the E-voting system can be made secure by making it fully transparent and stopping vote duplicity. It suggested that one should use smart contracts which will allow a user (address) with valid EOA's to vote only once. But, this concept lacks true automated address verification protocol as the EOA's get their voting rights from a central authority to be an eligible voters. It mainly offers business rules transparency and single vote restriction per EOA.

During discussion over the paper by TarasovET. Al [10] we came to know about E-voting and its use with blockchain. The solution proposed by them is a registration phase which will verify the users identity in addition to blockchain DAPP's inherent properties like transparency, privacy and integrity. First step is the registration which is done for verifying person's identity for audit purpose which will keep track of voters who are casting ballot. Verification is done using challenge response handshake protocol, it consist of a server (central authority) to handle verification and adds user's data (email address) to the database. We all know that emails are relatively easy to spot.

During the discussion over the paper by Fernando Lobato Messer [11], it shows 2 types of ongoing issues with E-voting solutions. One is the process of result tallying from smart contract before the actual votes are casted and the others one is keeping the voters anonymous since the public keys can be associated with the votes that are casted or recorded. Author in his paper uses threshold keys and linkable ring structure over the smart contract which will be used to implement voting system. Nevertheless, it also consists a registration phase and the voters are dependent on a central authority for the registration of this public key for casting a vote.

A. Motivation

The problems associated with the current elections that are held in India are vote tampering, standing in lines for vote casting, capturing of booth etc. while all government elections and other organizational elections are done manually using paper ballots which are made confidential and are sealed, other polls and questionnaires'' are done sually over the Internet or SMS channels, votes are counted and announced publicly.

But the conventional paper-to-box voting system raises some issues like how reliable are the notaries at hand? How can we say that votes are not manipulated? How transparent is the election? How can we make voters trust the election system's transparency? How costly can elections be which is set up at one place with 1000 voters, including material, logistics and salary costs? What we can say about 1000 locations and 1000000 voters? And since elections take place every few years repeating all the setup for every election must cost much so what about that? These are some known problems and there are many more arising problems.

Since elections are easily manipulated or corrupted and votes can be tampered in small towns and even in big cities with corruption, it is important for us. Also elections can be very expensive since they are happening in large scale, in long term, especially if the voters and voting centres are distributed geographically. Also voters (mainly for members of organization) may not be present at the time of voting they might be on vacation or on a business trip which makes is impossible for that person to cast vote and it may affect the overall result and attendance.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Our main motivation towards this paper is to ensure a secured voting environment and showing that a reliable E-voting scheme is possible with the help of Blockchain. The democracy itself means providing all citizens with equal right and choose their representative in an unbiased manner. To completely digitalize the election over the Internet we resolve the following problems. We need transparency, authentication and probability in the voting platform. We need authentication of people that they are real and existing and are using correct credentials that we know in electronic environment and that should be 100% transparent. So, we require to collect and check signed and timestamps data of voting because nobody should be able to tamper with the votes after the casting is done. Elections require individuality so that no one can vote for other person.

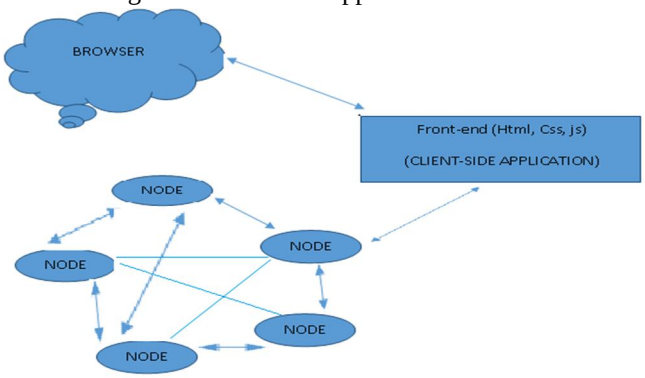
B. Proposed Solution

These issues can be resolve by Blockchain peer-to-peer technology. Defining the proposed self-executable smart contracts can be done. It is similar to writing code. We define rules, objects, data models and then contract can be executed. Once the smart contract are initialized, they can't be discarded from the blockchain and everyone can conclude whether execution results of smart contract are correct or not. Ethereum network doesn't require any central authority to provide proof-of-work. All peers are able to conclude the results of the contract without any interference.

C. Our Dapp Structure

We have a client side application and instead of connecting this to a back-end server we will connect it to the local Blockchain that we will install and we will write all the code to our DAPP Smart contract. We will compile our Smart contract and deploy it to our local Blockchain and we will allow accounts in the network to use our app and vote in the election.

Fig 1: Decentralized application structure.



D. Implementation Details

Contracts are written in Solidity programming language, which is a blend of C++ and JavaScript. The Ethereum Virtual Machine (EVM) is utilized as the Blockchain runtime condition, on which straightforward, steady and deterministic savvy contracts will be sent by coordinators for each casting a ballot occasion to run the casting a ballot rules.

Before going further for coding we have to download some dependencies (node package manager, truffle framework, ganache, metamask extension for google chrome).

Open ganache [12]. Download pre-defined functions using truffle unbox pet-shop command. Now we listed the candidates of our election by writing the smart contract. With the help of command prompt migrate the smart contract and deploy it. Open truffle console to see the list of candidates and their information. We can also have access to ganache accounts in our console and we do this with a library called web3. So, now let's write the code that allow us to list out the candidate on our client side application. In order to do this we are going to write some html and some JavaScript code. Now open node.js command prompt and run the command npm run dev to see the result at client side. Now we have connected our front end application to the Blockchain, we can see the candidates that we created in our smart contract. We can see their names, we can see their vote counts and we can also see the account that we are logged into in metamask to our local Blockchain. Next we want to add in our Smartcontract the ability to cast the vote. To cast the vote we will go into our Smartcontract and we will define our voting function. Let's jump into the console and try to actually cast a vote with the function that we have just created. Now we will allow an account to vote using our client side application.

©IJRASET: All Rights are Reserved

III. RESULTS

Fig 2: We can cast vote using vote button which we can see on the web page while the voter is logged in with its private account.

Fig 3: we can see that as we cast our vote which is kind of a transaction the ether of the account which has casted the vote reduced by some value which shows that writing costs.

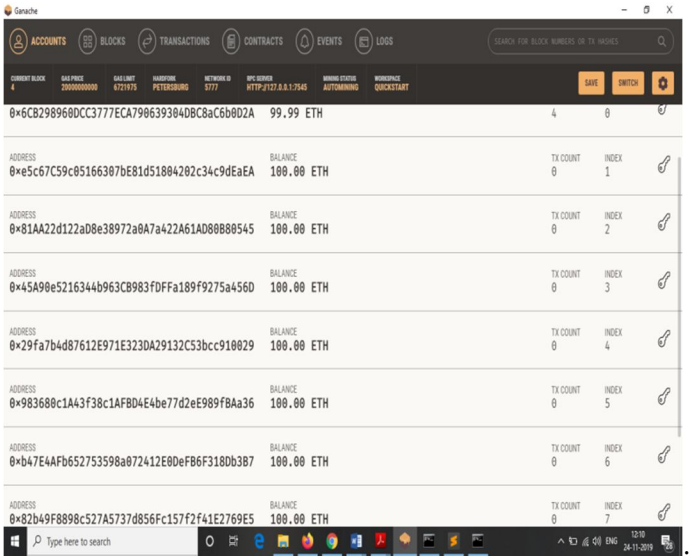


Table 1: comparison with existing system

Estonia E-Voting System	E-VOTING Using Blockchain Technology
• Id-cards are used voter identification. • Possibility of re-vote. E-voter can cast his/her vote again and the previous vote will be deleted. • If a voter votes both from poll and online then the priority will be given to the vote casted at the polling booth.	• Digital accounts are used for voter identification. • Voters can't revote by the same account. So there will be no manipulation. • Only online voting is valid and you can cast vote from anywhere.

©IJRASET: All Rights are Reserved

IV. CONCLUSION

A peer to peer network is created to present a private blockchain that share this distributed ledger having voting transaction. Each voter is uniquely identified by its address. Single voter can't vote twice using the same account. No single entity on the network can manipulate the code and the votes. So using blockchain technology we have formed a secure and transparent E-voting system.

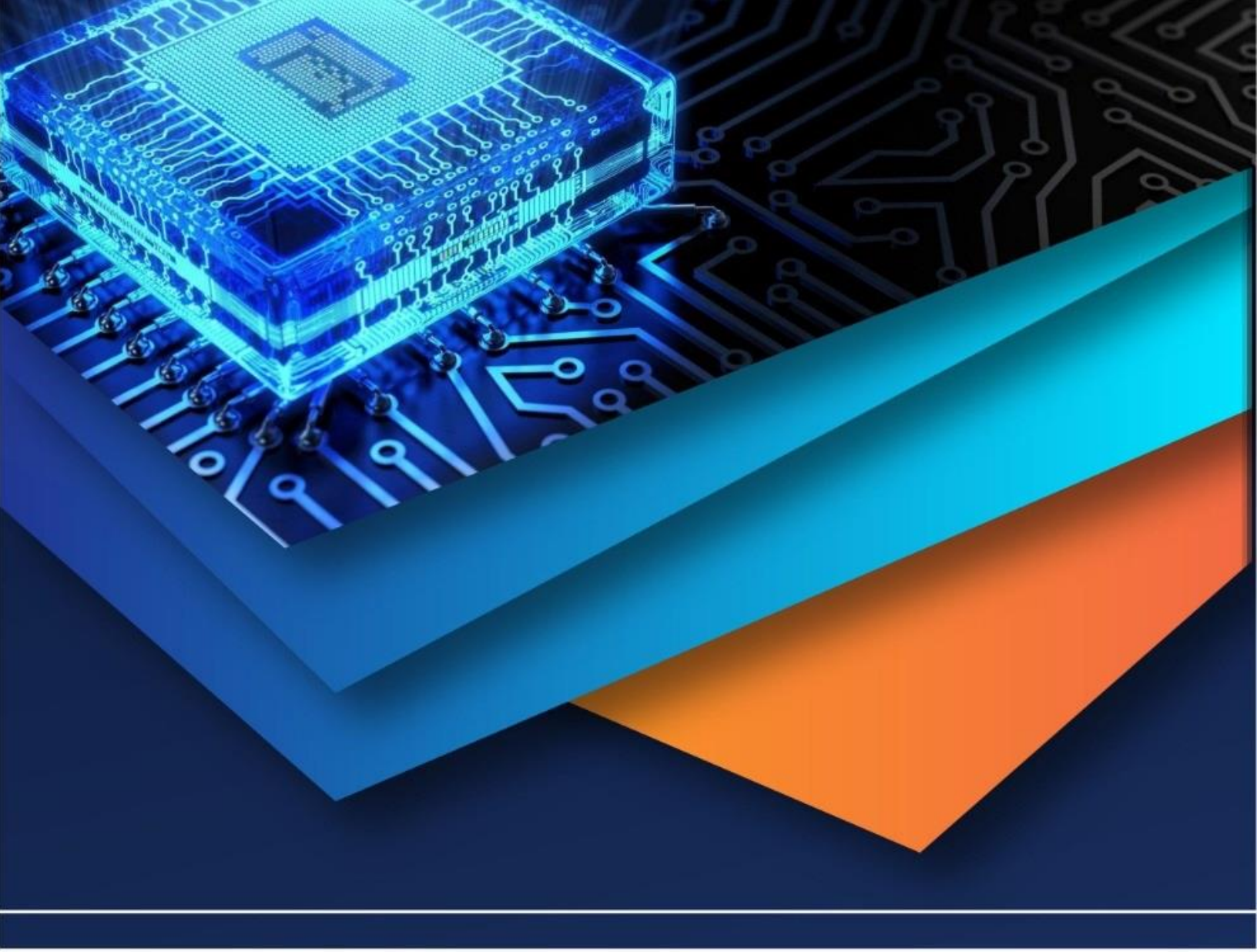
V. FUTURE SCOPE

The user interface and results visualization could be customized and adapted to the customer requirements. This system could be improved further So that it could be more secure and reliable for national government elections, which uses fingerprint or a special device located in the voting centres. Generally the statistics and reports are formed using general properties like sex, area, age,etc. What we can further add is their adhaar APIs which would be more significant.

REFRENCES

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system".
[2] https://blockgeeks.com/guides/smart-contracts/
[3] https://blockgeeks.com/guides/what-is-cryptocurrency/
[4] Ethereum white paper, https://github.com/ethereum/wiki/wiki/White-Paper.
[5] E. Maaten, "Towards remote e-voting: Estonian case", Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.
[6] N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. GesellschaftfürInformatik, Bonn, pp.43-52, 2004.
[7] Follow My Vote: https://followmyvote.com/online-voting-platformbenefits/open-source-code/.
[8] Andrew Barnes, Christopher Brake, Thomas Perry, "Digital Voting using Blockchain technology", https://www.economist.com/sites/default/files/plymouth.com
[9] A. K. Koc¸ and U. C. C¸ abuk, "Towards secure e-voting using ethereum blockchain."
[10] P. Tarasov and H. Tewari, "The future of e-voting." IADIS International Journal on Computer Science & Information Systems, vol. 12, no. 2, 2017.
[11] F. L. Meeser, "Decentralized, transparent, trustless voting on the ethereum blockchain," 2017.
[12] https://www.tutorialspoint.com/ethereum/ethereum_ganache_for_blockchain.htm

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)