International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

E-Voting using a Decentralized Ethereum Application

V. Arun, Aditya Dutta, Sourav Rajeev, Rohan Varghese Mathew

Abstract - As technology progresses with each passing day, its impacts only become more positive. One such outcome is blockchain. It has the potential to revolutionize the process of voting due to its decentralized nature and property of immutability. Voting in most places is a very non-transparent process and is known to be rife with corruption. With the introduction of blockchain as a service in the voting sphere, a potential protocol can be created such that the process of voting is completely open, fair and independently verifiable by anyone. Moreover, this paper elucidates the potential of a distributed ledger using a case study and aims to highlight the pros/cons of using blockchain architecture as a practical application in the process of voting.

***Index Terms*: Blockchain, decentralized, distributed, e-voting, ledger**

I. INTRODUCTION

In today's world, where everything revolves around technology and the internet, it remains to be asked as to why our election services remains out dated and almost obsolete. The idea of E-Voting is not a new one, but the procedure to implement the idea is challenging. By bringing in the concept of E-voting, there are numerous advantages. No more queuing up for voting and which results in a greater number of people willing to participate. Considering the existing system where the voters have to be present at the polling booth where they receive an admit ticket that then allows them to cast a vote, the entire process of voting within a particular area depends on the integrity of the person overseeing the elections. So, the process is not exactly fool proof. The proposed system brings in a considerable increase to security and integrity. A person will be able to cast his vote virtually from his home where his/her identity will be verified online. He/she can further check to see if the vote cast is successful or not.

This is done by applying the concept of blockchain that brings with it a considerable amount of added security and transparency to the current system. The decentralized and distributive nature of blockchain are the key features on which the whole system is based upon. Furthermore, the immutability of the system ensures that there is no scope of tampering as any and every transaction that has been recorded

has been done so permanently. This makes any form of modification impossible.

II. EXISTING SYSTEM

Electronic Voting:

Electronic Voting is the voting system where electronic devices are used to cast and count the votes. In this system, standalone Electronic Voting Machines (EVM). The common due process for this system of election is as follows -

1. Voters enter their personal information into the e-voting system.
2. E-voting system checks and validates the information entered by the user
3. After this is done, the voters cast their ballots, and their vote is stored securely.
4. The system then prepares to tally the votes.
5. The votes are counted and the final verdict is announced.

In general, there are two main types of e-voting:

1. Electronic voting (E-voting) that is supervised by election authorities in polling booths/stations.
2. Remote voting via the Internet (also called i-voting) is a process where the voter casts their votes online, remotely, that is from any location.

Documented Problems with E-Voting [1]:

Estonia:

Estonia introduced an online voting system in 2005, thus becoming the first nation to have such a system. The voters could cast their votes via the internet. The voters would need to download a voting application and authenticate their identities using their electronic ID. Upon examination, it was found that the system presented a number of problems including issues with transparency and security. The system was also vulnerable to Distributed Denial-of-service (DDoS) attacks.

Australia:

The system of iVoting was used in New South Wales in 2015. Findings revealed that around 66000 votes had been compromised. Although this system was deemed to be supposedly secure, experts believe that a third-party website was responsible for the attack.

India:

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
V Arun*, Computer Science & Engineering, SRM Institute of Science & Technology, Chennai, India.
Aditya Dutta, Computer Science & Engineering, SRM Institute of Science & Technology, Chennai, India.
Sourav Rajeev, Computer Science & Engineering, SRM Institute of Science & Technology, Chennai, India.
Rohan Varghese Mathew, Computer Science & Engineering, SRM Institute of Science & Technology, Chennai, India.

In 2017, in Rajasthan, it was found that eighteen EVMs were registering votes for the wrong party. There have been several similar cases in the country.
Malaysia:
E-Voting was used in the 2018 elections. Due to several technical problems, the elections had to be postponed several times.
Considering the aforementioned examples, it can be said that the E-Voting system poses the following threats.
1. The existing system is not transparent. There is no surefire way of checking if a voter's vote has been recorded in the main database or not.
2. It is not secure as there have been many instances where the confidential information of the voters was leaked.
3. The current sphere of voting is not an open process. Its internal workings are accessible only to certain people as opposed to it being open to the public.
4. A power-hungry organization can easily manipulate the system.
5. The current election process is a very expensive affair that requires heavy prior planning, organization of police officials and other election officials.

III. PROPOSED SYSTEM

As we know, the current existing system is riddled with many problems that lead to a very inefficient process of voting. Thus, the voting system that is hereby conceived must satisfy the following requirements –
1. The election system must be openly verifiable and transparent.
2. The election system must ensure that the vote cast by the voter has been recorded.
3. Only eligible voters must be allowed to vote.
4. The election system should be tamper-proof.
5. No power-hungry organization must be able to manipulate and rig the election process.
Using a Blockchain, the most important requirements are satisfied –
1. Authentication – Only registered voters will be allowed to vote.
2. Anonymity – The system prevents any interaction between the votes casted by the voters and their identities.
3. Accuracy – Votes once cast are permanently recorded and cannot be modified or changed under any circumstances.
4. Verifiability – The system will be verifiable such that the number of votes is accounted for. [4]

IV. SYSTEM ARCHITECTURE

Blockchain:
Satoshi Nakamoto first introduced the concept of Blockchain in 2008 during the cryptocurrency boom of the Bitcoin. It can be said that the Bitcoin was the first real implementation of Blockchain.
A Blockchain is a distributed and decentralized public ledger. The PoW (Proof of Work) protocol is the consensus protocol that used in the blockchain. The chain that is so formed as a result of mining in return for financial incentives is publicly and openly verifiable. It is cryptographically secure such that the data once written onto the Blockchain is tamper-proof. The immutability property of the Blockchain is done in such a way that once a new block has been appended to the Blockchain, it is recorded permanently and cannot be changed whatsoever. [8]
There are several types of Blockchains depending on the situation and the requirement –
1. Permissionless Blockchain – It does not require any permission and is open for all. Anyone can be a user and anyone can read/write a node. Anyone can also participate in a consensus to determine the state's veracity.
2. Permission Blockchain – It is opposite to a Permissionless Blockchain where the Blockchain is operated by stakeholders or members of a consortium. The type of Blockchain has the means to identify nodes that can read, control and modify data. Parties that can issue transactions can also be controlled this way.
3. Private Blockchain – It is a special type of Blockchain that is controlled only by one entity. These kind of blockchains are used in cases where the participants required need to be of the same organization.
In the Proposed System, we will use a permissioned blockchain, a consortium-based chain that uses the proof-of-authority consensus algorithm. [4]

A. Hash Functions:
The integrity of a blockchain is maintained using a blockchain. Using this hash function, each block is processed one by one where a hash from the previous block is connected. For the block to be accepted unanimously, it must have the correct hash value from the previous node and for the current node. [5]

B. Digital Signature:
Digital signatures provide a layer of authentication in the blockchain. Every valid signature consists of two keys. A private and a public key. The private key provided access to all the information that is stored in the account and is confidential and must not be shared with anyone. The public key can be shared with anyone and it is also used to initiate transactions in the blockchain. [5]

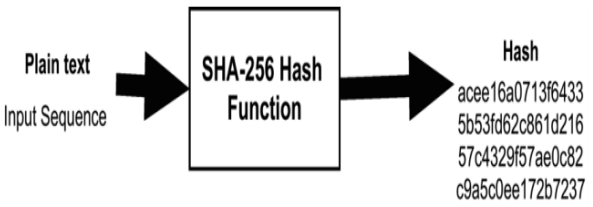

Fig 1. Basic Node in a Blockchain

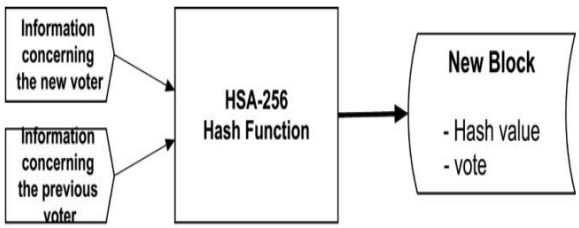

Fig 2. Linking of nodes using hash functions

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

V. IMPLEMENTATION

The implementation consists of:
Frontend:
1. Interface is provided by Metamask, a Google Chrome plug-in.
2. One HTML/CSS & Bootstrap page.
3. Two scripts written in JavaScript.
Backend:
1. Two smart contracts coded in Solidity.
2. Truffle Suite (Ganache) provides a personal, modifiable Ethereum blockchain.
Frontend:
The frontend provides an interface to the user such that it is possible to view and interact with data using the frontend languages, HTML/CSS and JavaScript.
Metamask –
Metamask is a Google Chrome plug-in that was designed to make the Ethereum Blockchain more accessible to users. It acts as an Ethereum browser where users can manage their decentralized applications, digital wallets and smart contracts without having to run a full-scale installation of the blockchain. Metamask along with Web3, an authentication protocol together ensure that users have a high level of security while performing transactions and do not have to run a full-scale node system. [2]

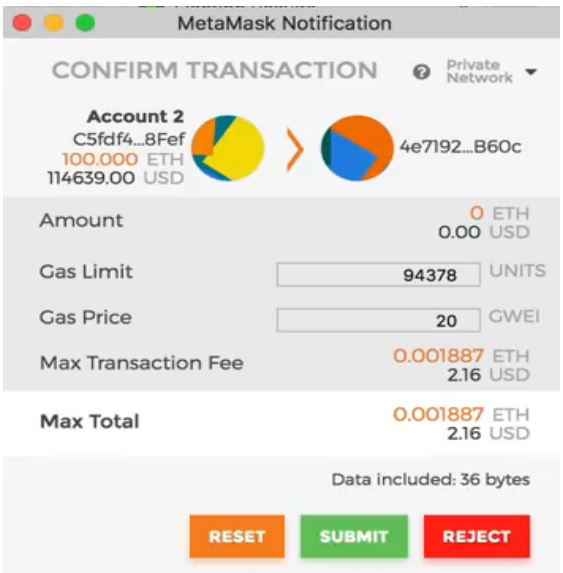

Fig 3. Transaction Confirmation

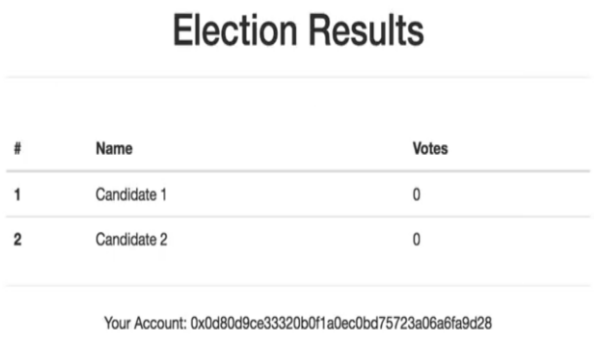

Fig 4. User Interface

Index.html –
This file is coupled with CSS and Bootstrap to provide the user interface for the voters. In this page, voters can cast and confirm their vote and they can see the real-time result of the vote. The file App,js is invoked after the introductory steps are finished. [9]

App.js –
The App.js file consists of the primary logic and computes the addition of the voters. It gathers information from Index.html and is used for storage.
Truffle-contract.js –
This JavaScript file connects and links the Smart Contract logic files to the frontend user interface.
Backend:
The backend deals with authentication, security and data storage of the implementation. Solidity is the programming language used to code in the Backend.
Election.sol –
This Smart Contract acts as a spawner for the election candidates. It acts as a virtual ballot and regulates the whole election process. It also tracks all the candidates to perform voter verification.
Migration.sol –
This is a secondary Smart Contract file that maintains all the migrations that occur each time the blockchain is reset and restarted. It ensures that for every fresh iteration, the candidate values are reset to zero.
Truffle Suite (Ganache) –
Ganache is a personal Ethereum blockchain which can be used to issue and execute commands, perform testing and inspect the state of the blockchain.

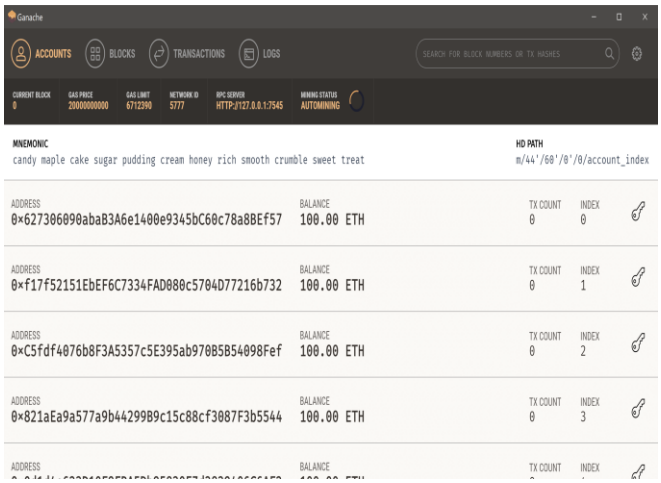

Fig 5. Personal Ethereum Blockchain

VI. CONCLUSION AND FUTURE WORK

Despite various advancements in technology, it is evident from the presentation that the current voting system is not fool-proof. It can easily be bypassed in order to favor one party or candidate. This is due to the fact that there is a blatant lack of transparency in the system.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Corruption in the voting process would undermine the very pillar on which a democratic government is built. The current system depends on a lot of man power to ensure that the votes are not tampered with.

Using blockchain as a backend in the election process, transparency can be ensured. The voter can therefore be assured that his vote cannot be tampered with. Implementing the system of blockchain into the voting process also ensures anonymity. This system also eliminates the need for a third person as the vote is directly recorded in the system. These improvements to the existing voting system would not only safeguard the voter's vote, but this would also result in greater turnouts in the election booths as the voters can know for sure that their vote will be recorded.

For future work, we look to expand the scope of this system where we can accommodate a large number of users and more forms of voting.

Additionally, we look to bolster our system of cryptography where we use third-party libraries in Solidity to generate specific keys for every ballot. This prevents other ballots from being compromised.

REFERENCES

1. Ahmed Ben Ayed, 'A conceptual secure blockchain- based electronic voting system', International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017
2. Gaby G. Dagher, Praneeth Babu Marella, 'BroncoVote: Secure Voting System using Ethereum's Blockchain', Boise State University, Boise, Idaho, USA, 2018
3. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, 'Blockchain-Based E-Voting System' Reykjavik University, Iceland, 2018
4. Rifa Hanifatunnisa, Budi Rahardjo 'Blockchain Based E-Voting Recording System Design', Bandung Institute of Technology, Bandung, West Java, Indonesia, 2017
5. Clement Chan Zheng Wei, Chuah Chai Wen, 'Blockchain-Based Electronic Voting Protocol' University Tun Hussein Onn Malaysia, Malaysia, International Journal on Informatics Visualization (IJIV) Vol.2, No.4, 2018
6. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, 'E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy', University of London, Egham, United Kingdom, 2018
7. Somnath Panja, Bimal Kumar Roy, 'A secure end-to-end verifiable e-voting system using zero knowledge based blockchain', Indian Statistical Institute, Kolkata, India, 2016
8. Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani and Andrea Pinna 'Crypto-voting, a Blockchain based e-Voting System' Piazza dArmi, Cagliari, Italy (2018)
9. Building an Ethereum Decentralized Application -http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial

AUTHORS PROFILE

V. Arun, is an Assistant Professor at SRM Institute of Science & Technology. He has over 10 years of experience in teaching. He got his Bachelor's Degree in Computer Science & Engineering from SA Engineering College and Master's degree from Rajalakshmi Engineering College. Main area of research interest is Big Data and Data Mining.

Aditya Dutta, is an Undergraduate Scholar pursuing Computer Science & Engineering from SRM Institute of Science and Technology. He is working under the guidance of Mr. V. Arun.

Sourav Rajeev, is an Undergraduate Scholar pursuing Computer Science & Engineering from SRM Institute of Science and Technology. He is working under the guidance of Mr. V. Arun.

Rohan Varghese Mathew, is an Undergraduate Scholar pursuing Computer Science & Engineering from SRM Institute of Science and Technology. He is working under the guidance of Mr. V. Arun.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)