Decentralized Voting System

Sameer Agarwal[1], Vikrant S Bhalerao[1], Aman Agarwal[1], Pranav Naik[1], Murtaza Ziya[1], Milind Rane [2]

[1]*Electronics Department, Vishwakarma Institute of Technology, Pune, 411037, India.*
[2]*Professor of Electronics Engineering, Electronics Department, Vishwakarma Institute of Technology, Pune, 411037, India*
[1]*sameer.agarwal17@vit.edu, [1]vikrant.bhalerao17@vit..edu , [1]aman.agarwal17@vit.edu, [1]pranav.naik17@vit.edu, [1]murtaza.ziya17@vit.edu*
[2] *milind.rane@vit.edu*

Abstract— Blockchain is a technology that is based on Bitcoin cryptocurrency. It is a technology for decentralizing transaction and managing data. Immense research and deep thinking have gone into conceptualizing blockchain since the time it was first showcased by Satoshi Nakamoto in 2008. The growing interest among researchers and technologists is the central attribute of blockchain that provides a high level of security, anonymity and data integrity without any intervention from third party who is in control of the transactions. This research is aimed to design a decentralized E-Voting system. The core idea is to use blockchain technology in order to create a trustless voting system.

Keywords—Blockchain, Ledger, Decentralized Application, Smart Contract, Cryptocurrency**.**

INTRODUCTION:

Blockchain is a distributed database which maintains a list of records that goes on increasing continuously known as blocks that are secured from tampering and revision. Every block contains a timestamp and is a link to the previous block. The blockchains are designed in a fashion such that they are inherently resistant to the modification of data. Blockchain utilizes a peer to peer network, a distributed time-stamping server and tamper-proof records of transaction data that makes it even more secure and helps to order data in a much organized way. The technology of blockchain is an open, distributed ledger which can track and record transactions taking place between a buyer and a merchant or simply between two parties involved in an efficient approach. Algorithm now days are efficient enough to trigger transactions automatically which is almost like an evolution in the banking world. The network, design architecture and an example of a distributed computing system with high fault tolerance have almost opened the gateway of the world especially in the financial sector. Thus, decentralized consensus can be achieved with blockchain making it suitable for identifying and recording events, transaction processing and documenting provenance. In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of an electronic voting system, with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with new election system is critical to limit fraud and having the voting process traceable and verifiable.

General Election still uses a centralized system, there is one central server which holds and collects all the data. Some of the problem that can occur in a current electoral system is that a certain organization has full control of the database, and it is possible to tamper with it. A decentralized system provides public and transparent voting process while protecting the anonymity of voter's identity, the privacy of data transmission and verifiability.

BLOCKCHAIN TRANSACTIONS:

The significant advantage of blockchain is the method of transactions which are verified and trackable. Instead of having a trusted third-party or a central bank, the technology is based on consensus among a peer-to-peer network of computers that run on complex algorithms. Instead of storing in one database, time-stamped transactions in blocks are stored in different systems across a value chain. This helps in achieving a decentralization of trust which has helped realizing cross-border payments, trading and faster settlements in a reliable and cost efficient way. The key foundational elements of blockchain include:

- Decentralization – Distributing control among all peers in the transaction chain instead of having one central authority controlling everything within an ecosystem. Thus, the technology works on the principle of a shared infrastructure.

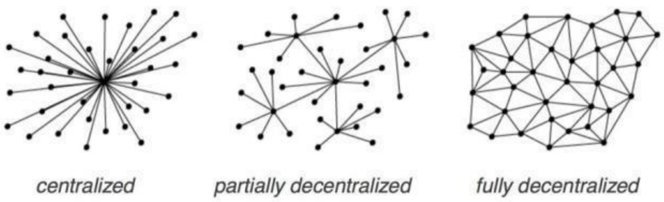


Fig. 1. Type of Ledgers

- Digital Signature- An exchange of transactional value using unique digital signatures that rely on public and private keys to create an authentic proof of ownership.
- Mining- After transactions are verified and completed, they are stored in blocks using strict cryptographic patterns.
- Data integrity- To prevent tampering of transaction data as agreed upon, the use of complex algorithm and consensus helps in ensuring data safety.
- Smart Contract- Smart contracts are trackable and irreversible applications that execute in a decentralized environment (e.g. Blockchain). Once the smart contract has been deployed nobody can edit the code or change its execution behavior. Smart contract guarantees to bind parties together to an agreement as written. This creates a new powerful type of trust relationship that does not rely on a single party. Smart contracts enable better management for realizing and administering digital agreements because they are self-verifying and self-executing.

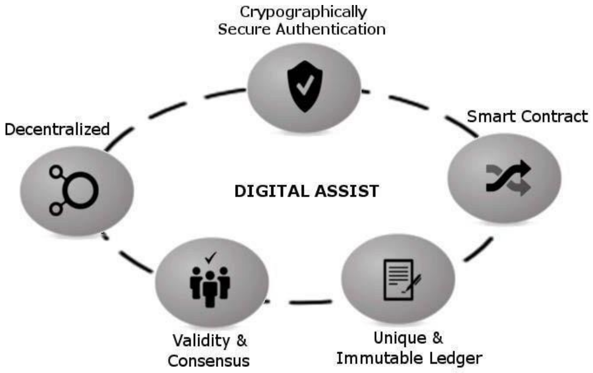

Crypographically Secure Authentication
Smart Contract
Decentralized
DIGITAL ASSIST
Validity & Consensus
Unique & Immutable Ledger

Fig. 2. Functional Components

Social Impact:

Recent major technical challenges regarding e-voting systems include, but not limited to secure digital identity management. Any potential voter should have been enrolled in the voting system prior to the elections. Their information should be in a digitally processable format. Besides, their identity information should be kept private in any involving database. A traditional voting system may face the following problems:

Anonymous vote-casting**:** Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

Individualized ballot processes**:** How a vote will be represented in the involving web applications or databases is still an open discussion. While a clear text message is the worst idea, a hashed token can be used to provide anonymity and integrity. Meanwhile, the vote should be non-reputable, which cannot be guaranteed by the token solution.

Ballot casting verifiability by (and only by) the voter: The voter should be able to see and verify his/her own vote, after he/she submitted the vote. This is important to achieve in order to prevent, or at least to notice, any potential malicious activity. This countermeasure, apart from providing means of non-repudiation, will surely boost the feeling of trust of the voters.

High initial setup costs- Though sustaining and maintaining online voting systems is much cheaper than traditional elections, initial deployments might be expensive, especially for businesses.

Increasing security problems: Cyber-attacks pose a great threat to public polls. No one would accept the responsibility if any hacking attempt succeeds during an election. The DDoS attacks are well known and mostly not the case in the elections. The voter integrity commission of the United States gave a testimony about the state of the elections in the US recently. Accordingly; Ronald Rivest stated that "hackers have myriad ways of attacking voting machines". As an example; barcodes on ballots and smartphones in voting locations can be used in the hacking process. Apple stated that we mustn't ignore the fact that computers are hackable, and the evidences can easily be deleted. Double-voting or voters from the other regions are also some common problems. To mitigate these threats, software mechanisms which promise the following should be deployed:

- Prevention of evidence deletion.
- Transparency with privacy.

Lack of transparency and trust: How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored.

Voting delays or inefficiencies related to remote/absentee voting: Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous.

The blockchain technology may address many issues regarding e-voting schemes mentioned in the above section and make e-voting cheaper, easier, and much more secure to implement. It is a considerably new paradigm that can help to form decentralized systems, which assure data integrity, availability, and fault tolerance. Some state that "the blockchain technology is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better." This technology aims to revolutionize the systems. The blockchain systems are formed as decentralized networked systems of computers, which are used for validating and recording pure online transactions. They also constitute ledgers, where digital data is tied to each other, called the blockchain. The records on the blockchains are essentially immutable.

Dependencies:

In order to build a decentralized application, we require few dependencies which are as follows:

- Node Package Manager (NPM)- It comes bundled with node.js. Node.js is an open source, cross-platform runtime environment for developing server-side and networking applications.
- Truffle Framework- Truffle is a framework that is going to allow us to create decentralized application on the Ethereum network. It's going to give us a suite of tools that allows us to write our smart contracts with the solidity programming language. It also gives us a framework for testing our smart contracts. It also gives us some set of tools to deploy our smart contract to the blockchain.
- Ganache- Ganache is a local and memory blockchain that we can use for all development purposes. It provides us with ten Ethereum sample account.
- Metamask- In order use the blockchain we must connect to it. Metamask is a special browser extension in order to be able to use the Ethereum blockchain. We will be able to connect to our local ethereum network with our personal account and interact with our smart contract by using Metamask.

Detailed Work:

First of all, we have to start Ganache. Once we have Ganache started, we have a local blockchain running. Ganache provides us with 10 accounts whenever it starts. And each of these accounts has a unique address and each account has been credited with 100 fake ether. Now, these account addresses are unique identifier that is going to represent our voter in the election.

Truffle framework gives us boxes which are packages of code that can be unboxed within our project to get us started faster. We have used the truffle pet shop box. This is box designed, especially for Ethereum. Now in the pet shop box we have different directories like 'contracts' where our smart contract will live and inside this directory there is a file 'migration.sol' which is going to handle our migrations whenever we deploy our smart contract to the blockchain. Below that 'node_module' directory this is where our node dependencies will live. We also have 'source' directory where we will develop our client side application. And a ‘test’ directory where we will keep all of our test files. Also, a truffle.js file which is the main configuration file for our truffle project.

After that, we made our smart contract, which is written in solidity. In this smart contract, we have listed all our candidates that will run in the election. We also have mentioned all the business rules that are going to govern our election namely like the fact that the account can only vote one time in the election. And also, the fact that each vote will be accountable for only one point. In the smart contract initial votes for each candidate has been set to 0. As someone votes for the candidate the count goes up.

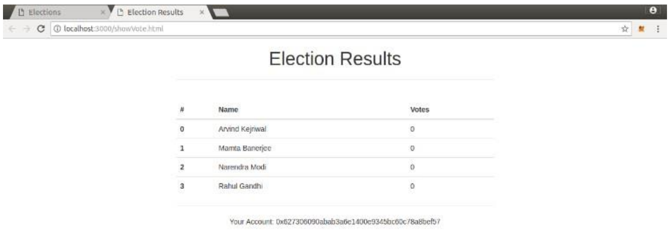
After the completion of our smart contract we migrated it to local blockchain. Migrations can be done only once because if we make some changes and migrate the contract again the blockchain loses its state and all the data is lost, hence proving the fact that blockchain is immutable. For client side of our application we wrote code in HTML and JavaScript.

Then we connected our client-side application to our local blockchain instance with help of Metamask extension. After connecting to the local blockchain network it generated the webpage shown in figure-2. In figure-2 below we can see the webpage of our admin-side decentralized application. Here only admin can register the voter candidate. As he registers a specific account id of some person that person can vote for the election. For voting, we have to import that specific account to Metamask so that we can vote.

Figure-3 is the webpage for our client where he can only see his account address. ‘Show Vote’ takes us to the webpage in figure-3 it counts all the votes and show vote counts of each candidate.

‘Declare Winner’ button basically counts all the votes after the voting has done and announces a winner.

Figure 1

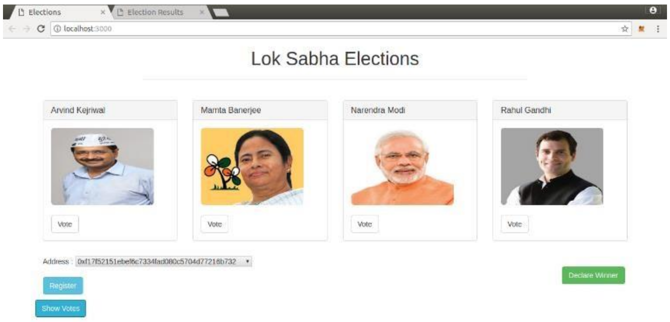


Election Results

#	Name	Votes
0	Arvind Kejriwal	0
1	Mamta Banerjee	0
2	Narendra Modi	0
3	Rahul Gandhi	0

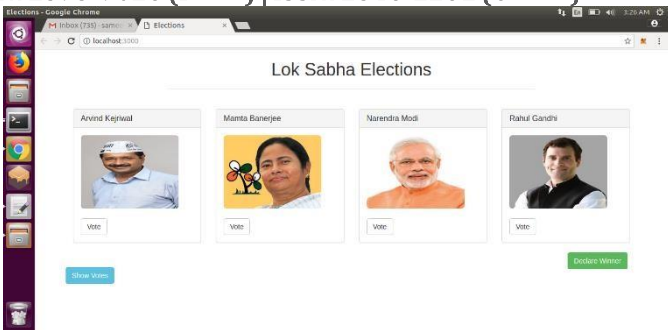
Your Account: 0x627306090abab3a6e1400e9345bc60c78a8bef57

Figure 2



Address : 0xf17f52151ebef6c7334fad080c5704d77216b732

Figure 3



CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and security analysis of the system. By comparison to previous work, we have shown that the 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 today’s scheme and offer new possibilities of transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voter’s vote is counted from the correct district, which could potentially increase voter turnout.

Result

With the decentralized application that we have made in this project, we were able to successfully create a local private blockchain. Demonstrate how blockchain can revolutionize our IT industry with different application. And show the successful working of our ‘Decentralized Voting System’.

References

[1] Ahmed Ben Ayed(2017); A Conceptual Secure Blockchain – Based Electronic Voting System; International Journal of Network
Security & Its Applications (IJNSA) Vol.9, No.3,

[2] Pavel Tarasov and Hitesh Tewari(2017); The Future of
E- Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I

[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3(2017); An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.

[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review; PLOS-ONE.

[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Cryptocurrency; Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[6] Michael Crosby, Google, Nachiappan, *Yahoo,*Pradhan Pattanayak, Yahoo, Sanjeev Verma, Samsung Research America,Vignesh Kalyanaraman, Fairchild Semiconductor(2015); Blockchain Technology Beyond Bitcoin.

[7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR]

[8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim(2016); Electronic Voting Service Using Block-Chain; Journal of Digital Forensics, Security and Law.

[9] Aayushi Gupta1*, Jyotirmay Patel2, Mansi Gupta1, Harshit Gupta1(2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017)

[10] Gautam Srivastava1, Ashutosh Dhar Dwivedi2 and Rajani Singh2(2018); Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology.

[11] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson(2018);Blockchain-Based E-Voting System.

[12] Nir Kshetri and Jeffrey voas(2018); Blockchain Enabled E-Voting;www.computer.org/software.

[13] Umut Can Çabuk1, Eylül Adıgüzel2, Enis Karaarslan2(2018); A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems; International Journal of Advanced Research in Computer and Communication Engineering.

[14] Madise, Ü. & Martens, T. (2006). E-voting in Estonia 2005. The first practice of countrywide binding Internet voting in the world. Electronic Voting, 86.

[15] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol,
California (2016).

[16] Jason Paul Cruz1, a)Yuichi Kaji2, b)(2017) E-voting System Based on the Bitcoin Protocol and Blind Signatures; IPSJ Transactions on Mathematical Modeling and Its Applications Vol.10 No.1 14–22.

[17]https://www.google.com/A+Simple+Representation+of+the + Blockchain+Structure+of+each+Candidate+in+e+2163oting

[18] Vikrant S Bhalerao is currently pursuing his bachelor's degree in Electronics Engineering from Vishwakarma Institute of Technology, Pune.

[19] Sameer Agarwal is currently pursuing his bachelor's degree in Electronics Engineering from Vishwakarma Institute of Technology, Pune.

[20] Aman Agarwal is currently pursuing his bachelor's degree in Electronics Engineering from Vishwakarma Institute of Technology, Pune.

[21] Pranav Naik is currently pursuing his bachelor's degree in Electronics Engineering from Vishwakarma Institute of Technology, Pune.

[22] Murtaza Ziya is currently pursuing his bachelor's degree in Electronics Engineering from Vishwakarma Institute of Technology, Pune.

[23] Milind Rane is currently a Professor in Department of Electronics Engineering, Vishwakarma Institute of Technology, Pune