International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

Electronic Voting System Using Blockchain

Ritika Singh[1], Riya Chaudhary[2], Adarsh Tripathi[3]

[1]*Assistant Professor, Department of CSE, SRM Institute of Science and Technology, Ghaziabad*

[2]*Department of CSE, SRM Institute of Science and Technology, Modinagar, Ghaziabad*

[3]*Department of CSE, SRM Institute of Science and Technology, Modinagar, Ghaziabad*

ABSTRACT

Blockchain is a system that records information in such a manner which renders it difficult and nearly-impossible to create changes. Blockchain technology provides a very wide range of applications in benefitting from sharing economy.Using that we'll quantify the applications of blockchain as service to carry out distributed electronic voting system. General elections in our country still use a centralized system for their process of voting. There is one organization that is dedicated to manage it. There is one major problem in this system. The full-control of a single organization over the complete database and system is the major complication that occurs in a normal electoral system.The vote counting in traditional system may take days and thereby elevating the cost of election.[1] **It is very much possible to modulate the database of opportunities worth consideration. We now present an Electronic Voting System based on blockchain which will eliminate each and every limitation that we found. To replace the traditional pen and paper voting method is very important to keep the frauds under control and make the voting process more transparent.**[2] **In any voting process, the most important element is 'trust', and this e-voting system guarantees it to a great extent.**[3]

More generally, this project appraises the competency of distributed ledgers technology through the explanation of a case study, namely the method of conducting an election and implementing a blockchain-based application which enhances the security of the system.

General Terms

Blockchain Technology, Ethereum Cryptocurrency

***Keywords*-** Blockchain, Distributed General Ledger, Ethereum, Electronic Voting System, Smart Contracts, liquid democracy, Decentralizedsystem[1], Transparent, P2P network, Immutable, Distributed, Inconvertible, Consensus Algorithm, PoW Algorithm, PoS Algorithm, Decentralised Application

1.INTRODUCTION

A blockchain is node to node interconnected system. Each node has many blocks. Each block consists of three parts, Hash, Data, and Previous Hash.(Fig 1)

Every hash is data specific. So in-order to change a particular data, we need to change its corresponding hash in the next block, As a hash is data specific, any change in a hash will cause its corresponding data to change, which is practically not possible. Due to the above stated reason, the blockchain technology is said to be immutable.

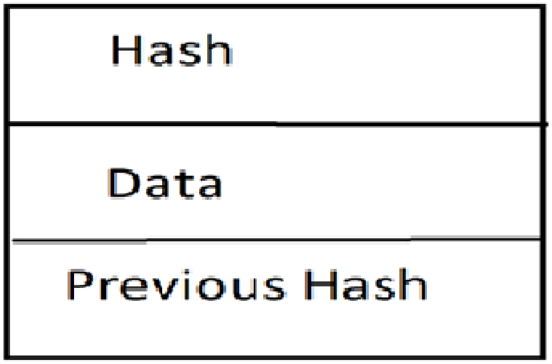

Fig 1

General elections in a country still use centralized systems for their process of voting. There is one and only one organization that is dedicated to manage it. There is one major problem in this system. The full-control of a single organization over the complete database and system is the major complication that can occur in normal electoral systems. Thereby, by using a block chain, we can create a decentralized system which is way more secure and reliable than a centralized system.

We have tried to make a system using which an eligible voter of a country can cast his valuable vote just by making few clicks on his mobile or laptop. In this way, we have tried to create a system which is decentralized, reliable and cost efficient.

This is the reason why many people[4], not excluding us too, consider blockchain technology as a ground-breaking tool for the voting process.

Fig 2 gives a symbolic representation of blockchain.

BLOCK
CHAIN
BLOCK
CHAIN
BLOCK

Fig 2

2.LITERATURE SURVEY

In early eighties, David Shaum created the first ever e-voting system, which made use of cryptography (public key) and the voters casting the vote were kept anonymous.

Furthermore, research done by RifaHanifatunnisa stated that expense can be more effectively managed if the hardware required for casting the vote doesn't need to be dynamically changed with the changing conditions like area, type of election (like a state election or Election for Mayor in a particular city)[5]

Research paper by s DivyaKamboj T. Andrew Yang investigates the use of blockchain for building framework for PC data. They additionally examined on how the innovation of blockchain profit framework training and in various instructions.[6]

Research work by Christian in 2017 emphasized on the number of days and time that a traditional ballot paper election system consume and the extent to which it can be reduced using the blockchain based voting system.[7]

The study by G Bhavani in 2018 states how blockchain technology can be one solution to solve the problems that often occur in the electoral system. The use of hash values in recording the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable.[8]

Paper by Kashif Mehboob Khan,Junaid Arshad, Mohd Mubashir Khan in May 2018 presents benefits of blockchain such as cryptographic foundations and transparency. The paper presents in-depth evaluation of the schemes which successfully demonstrates its effectiveness to achieve an end-to-end verifiablese-voting scheme.[9]

Paper by Rumeysa Bulut, Alperen Kantarcı, Safa Keskin and Serif Bahtiyar states security and data integrity of votes is provided theoretically. Voter privacy is ensured in the system. Waiting time for results is decreased significantly in proposed Blockchain voting system.[10]

The paper by Ahmed Ben Ayed states the drawbacks of the existing systems as the centralisation of systems is prone to DDOS attacks. By deploying open source code using blockchain the system will be decentralised making it more secure.[11]

Paper by Ong Kang Yi and Debashish Das proposes an Online Voting System that is Blockchain based to uplift the integrity, making the voting process optimized, producing voint results consistently, and strengthening the transparency of the voting system.[12]

Paper byFriðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa and Gísli Hjálmtýsson introduced a system that deploys all the uses of smart contracts to make the electronic voting systems based on blockchain more secure and ease the load on it.[13]

The paper by W.B. Liefhebber and M.L. van der Laan analysed the flaws of the existing systems and also the working of the blockchain leading to the conclusion that proper use of blockchain can solve many problems like tracking the actions, making data immutable and preventing recasting of votes among others.[14]

The paper by Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. MalatiV.Tribhuwan states the process of using different frameworks of blockchain technology to achieve advantages like eliminating tampering of votes by producing records that are secured cryptographically among various other ones.[15]

Paper by Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian and Amol Kharat presents the use of smart contracts to make a very secure and cost effective voting system that also provides privacy to the users. Ethereum network was found the most suitable for the deployment.[16]

Paper by Ruhi Tas and Ömer Özgür Tanrıöver presented an analysis of various other papers and hence concluded that the speed of transactions and protection of privacy are the problems most emphasized in the application of blockchain. Some frameworks need to be enhanced in order to make the application of blockchain more secure.[17]

3.PROPOSED ARCHITECTURE

The proposed system will consist of basically three parts Blockchain network (Having code implemented through smart-contracts), front end (I.e Client Side Application), and a browser.

The user will use his device to open a browser using which he will be able to cast his vote.
The user will be able to access the voting system from his own device. He just needs to have a metamask software installed on his system, which will enable him to connect to the blockchain network.
Fig 3 shows the proposed architecture of our system.

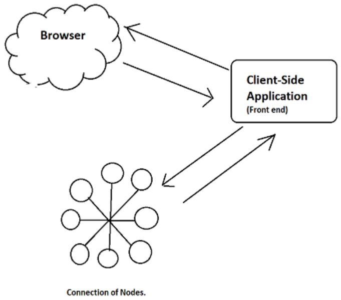

Fig 3

After proper authentication of the user, the eligible voters will be displayed a list of details candidates contesting the election. The user can then vote the candidate of his choice by clicking the vote button next to candidate name.
As soon as the user casts his vote, a few node, known as miners, will compete with each other to complete the transaction. The miners which finishes the transaction first gets the reward in the form of Ethereum Cryptocurrency known as ‘gas’.
The result will be updated as soon as the vote passes through smart-contract.
After the voter has voted his preferred candidate, logout button will be displaced. Now as soon as the logout button is clicked, the voter’s record will be deleted from the database. Now if the voter tries to re-login, in order to recast his vote, an error message will be displayed.
In this way we have prevented multiple logins from a voter, along with decreasing the data server size.

The architecture is used keeping in mind the idea of liquid democracy.
Liquid democracy is one in which the voter has the right to witness if the casting of his votes has been done to the candidate he intends. This way frauds can be reduced.[18]

3.1 BLOCKCHAIN ARCHITECHTURE

The voter will be able to access the voting system from his own device. The voter need to have Metamask software installed in theirweb browser. The user need to connect to special Ethereum network using network Id (IP address of the main Ethereum network). The device will join the main Ethereum network where smart contract is already present as per pre-defined protocols. The user will be able to send vote through metamask.The main Ethereum network will then process the vote as defined insmart-contract and vote will be stored in cryptographic form in theblockchain. The miners get reward for performing power consuming calculations. The result is updated as soon as the vote passes through smart-contract.
Figure 4 shows here the blockchain architechture.

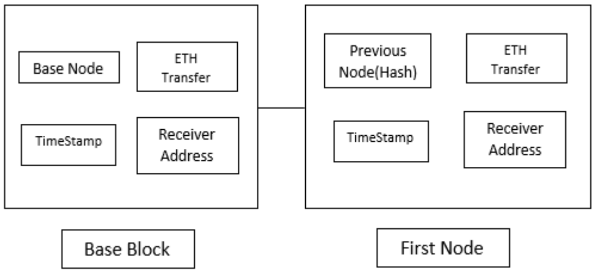

Figure 4

3.2 WEB ARCHITECHTURE

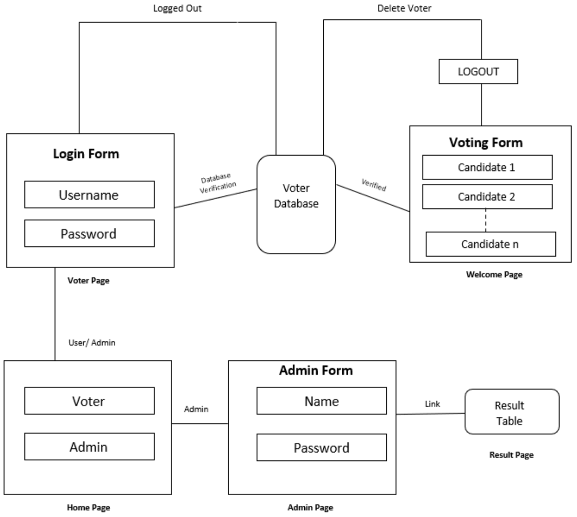

Figure 5

A user will be either a voter or an admin or both. As soon as the user will access the website he will see select whether he is a voter or he is an admin. If he is a voter he will select click on voter and a login form will appear in which he needs to enter credentials to login, and on submitting he will be taken to the welcome page but before that it will be verified whether he is an eligible voter or not. For this, his details will be verified against the Voter database to check his eligibility for voting, if he is eligible then only he will be taken forward to welcome page otherwise an error message will be displayed on the home page. Now in the welcome page , voter form will be displayed with the names and details of all the candidates of election. Voter will now vote for any one candidate and after clicking the button a pop-up will appear for logout and he will click the logout button.
Figure 5 here shows the web architechture.

4. CONCLUSION

EVM's are being used in India since years. Though the EVM technology proves more efficient than the ballot system, but the electronic voting will allow the users to caste their vote from their own devices and from the comfort of their home.[19] The use of block chain technology can provide mankind with the best solution to conduct elections in the most secure, transparent, flexible and cost-efficient way. The popularity of blockchain can easily be understood by the fact that this technology is being utilized by many crypto currencies, including bitcoin transaction framework.[20]The fact that, using this system, a user can cast his valuable vote from the comfort of his home by just making use of an electronic device will undoubtedly make sure that the election receives maximum vote input from eligible voters, and hence a majority of the population can decide whom they would like to elect as their leader and hence decide their fate.

5.METHODOLOGY AND ALGORITHM

We will deploy our Smart contracts using ethereum blockchain. The user just has to make sure that he has a Metamask Extension added to his browser.

Metamask extension connects the user to the ethereum network.

Ethereum allows us to write code that we can deploy on blockchain .[21]These codes will further be executed by the nodes on the blockchain. The high performance of Ethereum makes sure that least CPU resources are utilized thereby enhancing efficiency.[22]

Smart Contracts are responsible for reading and writing of codes, implementing business logic and transforming values. Smart Contracts are basically such conditions which must be fulfilled during the execution of our program.[23]Data tampering is also prevented in real time by Smart Contracts.[24]

The blockchain technology makes use of the Consensus Algorithm.

The consensus algorithm, according to the definition, means an accord in a group or party that has been accomplished in a dynamic fashion.[25]

Whenever a new block has to be added, it should be accepted by a majority of other blocks.

One such consensus algorithm is Proof-Of-Work algorithm.

To add a new block in the blockchain, the Proof of work algorithm entails solving a computationally difficult puzzle. This process is known as 'mining' and the nodes in the network that participate are referred to as 'miners'.

PoW works on the concept that the node which works more is likely to be less malicious and thereby more trustworthy.[26]

Apart from the above stated algorithm, we have also used a new method to prevent multiple logins from a same user. As soon as the voter casts his vote, his information is deleted from the database, instead of creating another database. If the user tries to relogin, he would face an authentication error and would not be able to caste his vote again.

6. FUTURE POSSIBILITIES

Voting systems have been around for a century and despite different opinions on their integrity, have always been deemed secure with few basic security and anonymity rules. Number of electronic systems have been presented and used but some suspicion
has been lifted regarding the integrity of elections due to detected security vulnerabilities within these systems. Electronic voting, to be successful requires a more see-through and secure way, than is offered spy current rules. The underlying technology used in the voting system is a paymentscheme, which offers anonymity of transaction's, a trait not seen in blockchain rules to date. The presented rules gives anonymity of voter transactions, while keeping the transactions private, and the election transparent and secure. The underlying payment rule has not been changed in any way; the voting protocol merely offers an alternative use case.

7. REFERENCES

[1] CEUR-WS.org, CEUR Workshop Proceedings (free, openaccess publishing, computer science/informationsystems/information technology), 2017.

[2] N. Weaver, Secure the Vote Today, 2006.

[3] J. Porup, Online voting is impossible to secure. So why are some governments using it?, 2018.

[4] TechCrunch, Liquid democracy uses blockchain to fix politics, and now you can vote for it Online., 2018.

[5] R. Hanifatunnisa and B. Rahardjo, “Blockchain Based E-Voting Recording System Design,” Vols. 978-1-5386-3546-9/17/$31.00, 2017.

[6] D. Kamboj and T. A. Yang, “An Exploratory Analysis of Blockchain: Applications, Security, and Related Issues,” *Int'l Conf. Scientific Computing ,* CSC'18.

[7] Christian, “Desain Dan Implementasi Visual Cryptography PadaSistem E-Voting Untuk Meningkatkan Anonymity,” *InstitutTeknologi Bandung,* 2017.

[8] G. Bhavani, “Survey on Blockchain Based E-Voting Recording System Design,” *International Journal of Innovative Research in Science,Engineering and Technology,* vol. Vol. 7, no. Issue 11, November 2018.

[9] K. M. Khan, J. Arshad and M. M. Khan, “Secure Digital Voting System based on Blockchain Technology,” *NED University of Engineering and Technology, Pakistan; University of West London, UK.,* May 2018.

[10] R. Bulut, A. Kantarcı, S. Keskin and S. Bahtiyar, “Blockchain-Based Electronic Voting System for Elections in Turkey,” *Faculty of Computer and Informatics Istanbul Technical University Istanbul, Turkey,* September 2019.

[11] A. B. Ayed, “A Conceptual Secure Blockchain- Based Electronic Voting System-,” *International Journal of Network Security & Its Applications (IJNSA) ,* vol. 9, no. 3, May 2017.

[12] D. D. Ong Kang Yi, “Block Chain Technology For Electronic Voting,” *Journal of Critical Reviews, ISSN- 2394-5125,* vol. 7, no. 3, 2020.

[13] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, “Blockchain-Based E-Voting System,” *School of Computer Science, Reykjavik University, Iceland,* July 2018.

[14] W. Liefhebber and M. v. d. Laan, “Defining an architecture for blockchain e-voting Systems,” *Utrecht University, Bachelor thesis - Information Science,* 7 July 2017.

[15] H. V. Patil, K. G. Rathi and M. V.Tribhuwan, “A Study on Decentralized E-Voting System Using Blockchain Technology-,” *International Research Journal of Engineering and Technology (IRJET), ,* vol. 5, no. 11, November 2018.

[16] A. Benny, A. A. Kumar, A. Basit, B. Cherian and A. Kharat, “Blockchain based E-voting System,” *Department of Computer Engineering, PCE, Navi Mumbai, India -410206.*

[17] R. Tas and Ö. Ö. Tanrıöver, “A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting,” *Computer Engineering, Ankara University, Turkish Radio Television Corporation, IT Department, Ankara, Turkey,* 9 August 2020.

[18] Nca.tandfonline.com, “Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties.,” 2015.

[19] https://www.indiatoday.in/, “Electronic Voting Machine: Here's all you wanted to know about India's EVMs.,” 2017.

[20] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[21] http://www.ethdocs.org/, “What is Ethereum? — Ethereum Homestead 0.1 documentation,” 2016.

[22] F. Vogelsteller, “https://github.com/ethereum/wiki/,” 2018.

[23] S. Ellis, A. Juels and S. Nazarov, “ChainLink: A Decentralized Oracle Network,” 2017.

[24] https://blokchainhub.net/smart-contracts/, “Smart Contracts,” 2018.

[25] https://blockgeeks.com/guides/smart-contracts/, “What Are Smart Contracts? A Beginner’s Guide to Smart,” 2018.

[26] M. Pilkington, “Blockchain technology: principles and applications,” 2015.