IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

# Towards Secure E-Voting Using Blockchain

Mishkaat Ansari, Mohammed Ahmed Shaikh **and** Yasra Ansari
Department of Computer Engineering
M. H. Saboo Siddik College of Engineering, Mumbai, India

**Abstract:** *Voting in this country is the most tedious job to be handled, involving all kinds of corrupted and illegal deeds. Elections in India are conducted exclusively using EVM's developed over the past two decades by a group of government-owned companies. These devices, known in India as EVMs, have been adopted greatly for their simple design, ease of conduct, and robustness. However, recently they have also been marked prey following widespread reports of election irregularities. Despite this criticism, many details of the mechanism have never been publicly discussed, and they have not been subjected to a stringent, independent security evaluation. We conclude that in spite of the machines' simplicity and software trusted computing base, they are vulnerable to indigenous attacks that can modify election results and violate the law of the election commission. Most of the attacks done are physical, by changing the electricals, but if the machine is connected real time to a cloud server and involves an independent screen which shows the confirmation of choice symbolically before placing the final vote, it can help in detecting problems and maintain the integrity of the system.*

**Keywords**: Blockchain, Decentralized system, EVM,Data security, IPFS, Encryption, Cloud storage.

**Blockchain:** A blockchain is a digitized, decentralized, public ledger of all crypto currency transactions.
**Decentralized system:** If one server goes down or something happens on a particular node, other nodes can function normally and do not have to wait for victim node's recovery.
**EVM:** The Electronic Voting Machine, also known as EVM, is an electronic device used for casting votes. The EVM aims to make the electoral process secure, fair and transparent.
**Data security:** Blockchain platform ensures that your data is encrypted, which means that modification in data is a difficult task.
**IPFS:** The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.
**Encryption:** The data encryption is a key technique in the blockchain technology. The way blockchain and encryption security works is based on math, through a mining network.
**Cloud storage:** In Blockchain-based cloud storage, data is divided into multiple encrypted segments that are interlinked through a hashing function.

## I. INTRODUCTION

Blockchain technology has primarily been used to store data and the major advantage of this technology is the inertia of the data. This technology was initially implemented by Satoshi Nakamoto in 2008 to imbibe the concept of cryptocurrency (or) bitcoins as a medium of secure electronic exchange of money. According to this technology the data once stored, a hash is generated, the following block stores this hash so as to form a chain of links between the data blocks. The hash generated is calculated from the data and any change in data causes the hash to change. The Proof-of-Work technology which is a part of the Blockchain technology, helps in preventing the modification of data by limiting the hashing rate. Hence, only a certain limited number of blocks can be created or modified at a time, hence lowering the chances of corruption. Moreover, the hashing in this case requires to be done at every peer node individually to be accepted by all the peers else it is rejected.

A blockchain is an audit trail for a database which is managed by a network of computers where no single computer is responsible for storing or maintaining the database, and any computer may enter or leave this network at any time

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

without jeopardizing the integrity or availability of the database. Any computer can rebuild the database from scratch by downloading the blockchain and processing the audit trail. The blockchain is a digital platform for digital assets. It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. Major usage of Blockchain has been in all cryptocurrency transactions, mainly Bitcoin. However, they are increasingly being used in a number of other applications because of their inherent resistance to modification to the transaction/block/whole distributed ledger - Blockchain. One such application is Electronic Voting. We will review some of the variety of blockchain technologies that are usable, scalable and secure, fit for Electronic Voting Application The simple explanation is a 'chain' of blocks. A block is an aggregated set of data. Data are collected and processed to fit in a block through a process called mining. Each block could be identified using a cryptographic hash (also known as a digital fingerprint). The block formed will contain a hash of the previous block, so that blocks can form a chain from the first block ever (known as the Genesis Block) to the formed block. In this way, all the data could be connected via a linked list structure.

Ethereum is an open platform that enables developers to build and deploy decentralized applications such as smart contracts and other complex legal and financial applications. You can think of Ethereum as a programmable Bitcoin where developers can use the underlying blockchain to create markets, shared ledgers, digital organizations, and other endless possibilities that need immutable data and agreements, all without the need for a middleman. Released in 2015, Ethereum is the brainchild of the prodigious Vitalik Buterin, who saw the potential uses of Bitcoin's underlying blockchain technology as the next steps in furthering the expansion of the blockchain community. Ethereum is now currently the cryptocurrency with the second highest coin market cap and is expected by some to surpass Bitcoin as both a valued investment and as the world's most popular cryptocurrency.

## II. Scope and Objective

It may help to establish e-voting systems as a reliables tool to conduct elections, already extensive research has been proposed. This project proposes an analysis of existing e-voting schemes along with their scopes and limitations.

- It satisfies the user requirement.
- Be easy to understand by the voter and operator.
- Have a good user interface.
- User friendly.

The objectives of the systems development and event management are:

1. It provides fault-tolerance, immutability, transparency and full traceability of the stored transaction records, as well as coherent digital representations of physical assets and autonomous transaction executions.
2. It is essential for the stored records to be tamper-proof, while the best case would be if each actor issuing transactions could do that without relying on any centralized third-party intermediary.

## III. Literature Survey

Existing System consist of methods like ballot paper-based voting, Lever voting machine, Punch card and EVM voting machine. The main problem with existing system was time consuming which used to take lot of time for voting. Paper based voting method were used in existing system which also gave the results of fake voting. Also, with EVM based voting there is lot of argument like EVM was hacked, So, such type of system is harmer for democracy country.

Disadvantages of Existing System:

- Lot of paper work required.
- Man power was more.
- Time consuming process.
- EVM may be hacked

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

| Title | Authors | Problem | Solution | Result |
|---|---|---|---|---|
| A Study on Decentralized E-Voting System Using Blockchain Technology | 1.Mrs. Harsha V. Patil, 2.Mrs. Kanchan G. Rathi, 3.Mrs. Malati V.Tribhuwan<br><br>Assistant Professor, Dept. of Computer Science, Dr. D .Y. Patil ACS College, Pimpri , Pune-18, Maharashtra, India | Vote rigging, hacking of the EVM (Electronic voting machine), election manipulation, and polling booth capturing are the major issues in the current voting system | The potential of the blockchain technology and its usefulness in the e-voting scheme. The blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. | The transparency of the block-chain enables more auditing and understanding of elections. |
| The Future Of Electronic Voting System Using Blockchain | Md. Razu Ahmed, F.M. Javed Mehedi Shamrat, Md. Asraf Ali, Md. Rajib Mia, Mst. Arifa Khatun | the traditional e-voting system has various limitations and challenges for a very long time. | The paper presents a novel secured distributed database of the voter's information, and voter information will be deposited against their private key and digital signature in the central database. | A Blockchain-based secure E-voting system that enables the decentralized database to cast vote in a modern way. |
| Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity | Chaitanya Rahalkar, Dhaval Gujar | The standard HTTP protocol has started showing its limitations. With an increased amount of data duplication & accidental deletion of files on the Internet. | A secured and integrity compliant system was proposed using the P2P feature of IPFS and the tamper-proof principle of Blockchain technology. | The four main components namely DHTs, Blockchain, P2P Networks and Content Addressed File System, together, make the model a secured, reliable, and fault-tolerant system. |
| **Decentralized Cloud Storage Using Blockchain** | Meet Shah, Mohammedhasan Shaikh,Vishwajeet Mishra,Grinal Tuscano | Cloud storage is one of the leading options to store massive data, however, the centralized storage approach of cloud computing is not secure. | the user's file is encrypted and stored across multiple peers in the network using the IPFS protocol. IPFS creates hash value. | This paper focuses on decentralized secure data storage, high availability of data, and efficient utilization of storage resources. |

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

## IV. PROPOSED SYSTEM

The proposed system has been designed and implements successfully using blockchain and fingerprint. The proposed system has the benefit of using a biometric authentication and controls the process of voting avoiding unnecessary things like rigging, ballot papers, casings etc.

We are going to design a system which is more secure, robust, and highly acceptable, more accurate and decentralized. So that no one can change anything in system, trust can be built by everyone. We are developing e-voting in blockchain. In our system, the admin can assign gas value to each voter for only one vote. Before assign gas value to voter and after giving the vote, the voter cannot vote in the system. Once voter can vote the data of the vote will uploaded on IPFS server and IPFS server generates the hash for that vote and that hash will maintained by Ethereum. In IPFS data are stored content-addressed and immutable, they can be complicated to edit.

Advantages of Proposed System:

- User friendly.
- No fake voting because of fingerprint.
- Transparency should be maintained.
- Reduce lots of paper work.
- Avoids invalid voting as it prevents unregistered voters from voting.
- Time conscious, less time required for voting & counting.
- This system allows only authenticated voting than the existing equipment as the person is identified based on his Fingerprint which is unique to each individual.

## V. METHODOLOGY

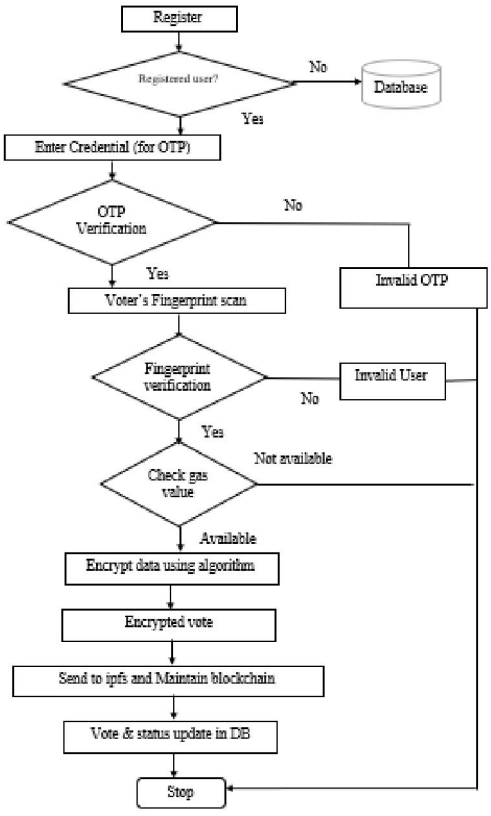



**Figure 1:** Flowchart

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

Initially if the user is new then he/she needs to register and the data will be stored in the database and if he is already registered then the system will ask for his credentials for verification. If the OTP is invalid then the process will stop else if the verification is successful then the system will ask for use's fingerprint. If the fingerprint doesn't match then the system will stop. After successful verification of fingerprint, the system will check gas value. The admin can assign gas value to each voter for only one vote and if the gas value is not available then the system stops. On the availability of gas value, blockchain uses digital signature (SHA256) algorithm to maintain/verify integrity of the data, this will encrypt the data. Once voter can vote, the data of the vote will be uploaded on IPFS server and IPFS server generates the hash for that vote and that hash will be maintained by Ethereum. At the end the status of the vote will get updated in the database.

## VI. ACTIVITY DIAGRAM

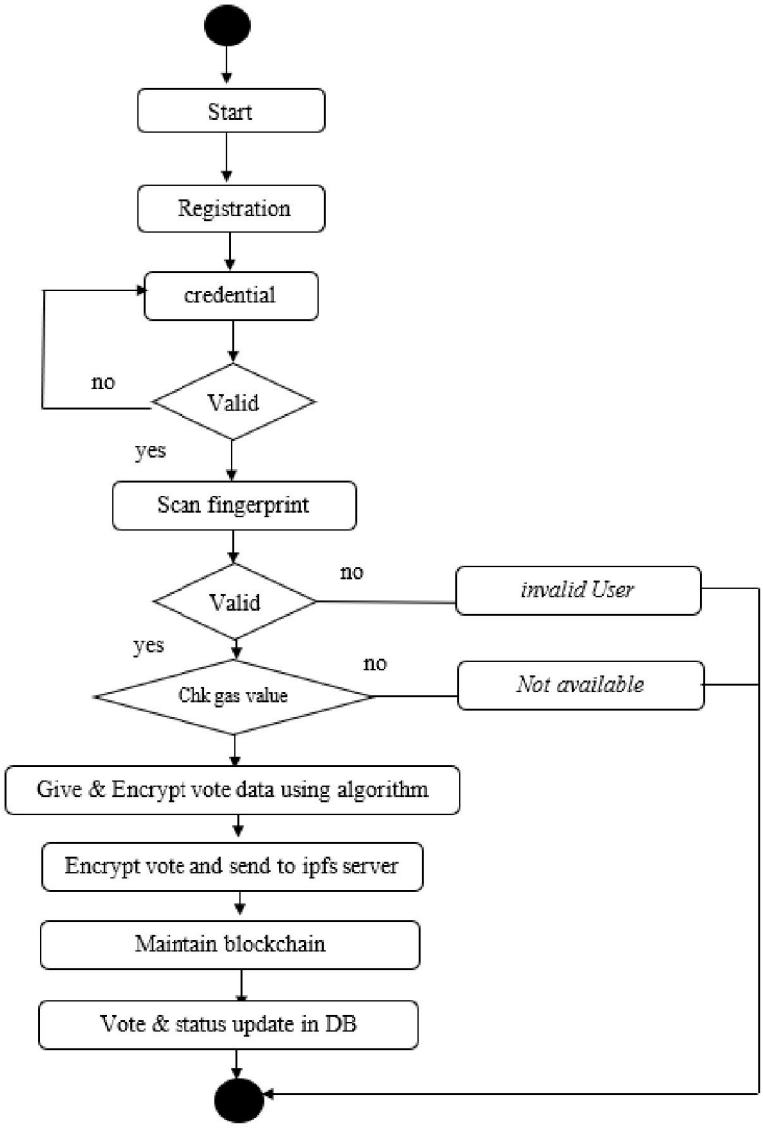



**Figure 2:** Voter Activity

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

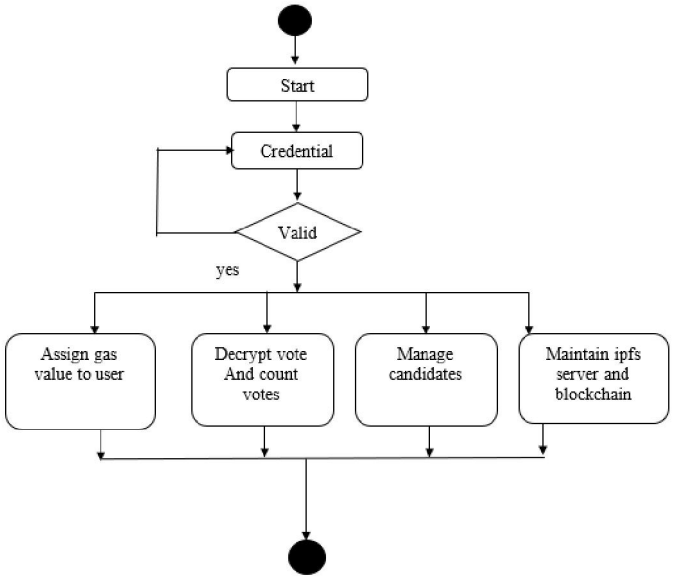
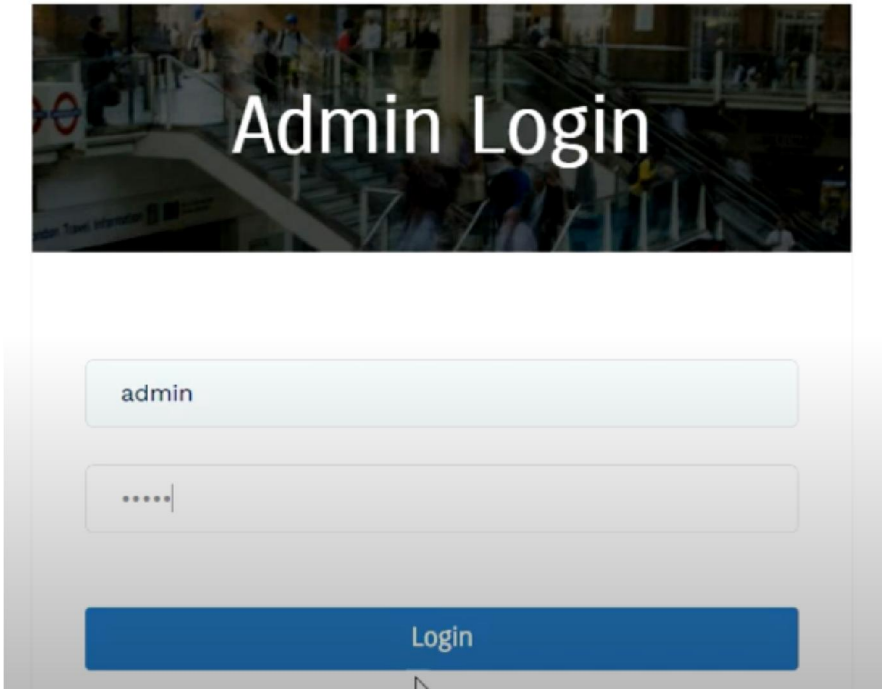
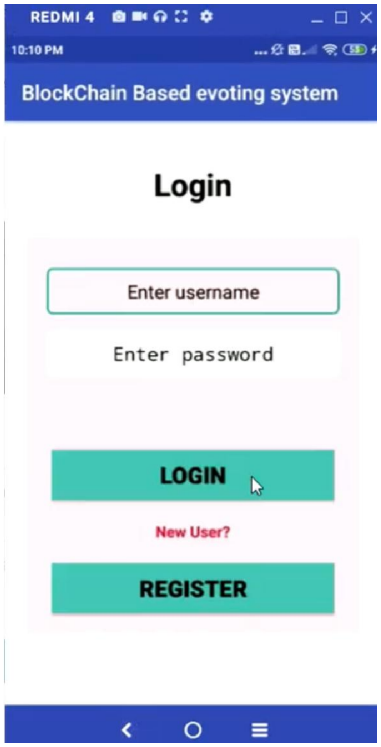


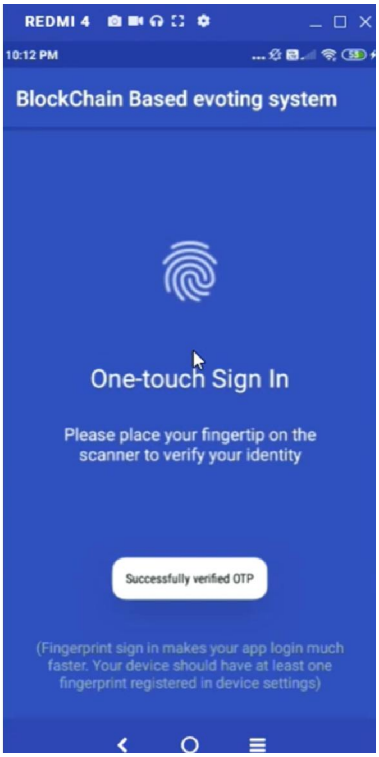

**Figure 3:** Admin Activity

## VII. RESULTS



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 5, Issue 1, May 2021
Impact Factor: 4.819

## VIII. CONCLUSION

In this project, 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 a 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. Implementing IPFS server-based solutions as well as blockchain for security will improvise on the transparency for the critics and also improve the security on the ballot information that is collected. Hence, the paper successfully demonstrates a way to improvise the political future in the country especially India.

## ACKNOWLEDGEMENTS

We wish to express our sincere thanks to our director Dr. Mohiuddin Ahmed and our principal Dr. Ganesh Kame, M.H. Saboo Siddik College of Engineering for providing us all the facilities, support and wonderful environment to meet our project requirements.

We would also take the opportunity to express our humble gratitude to our Head of Department of Computer Engineering Dr. Zainab Pirani for supporting us in all aspects and for encouraging with her valuable suggestions to make our project success.

We are highly thankful to our internal project guide Mohammed Ahmed whose valuable guidance helped us understand the project better, her constant guidance and willingness to share her vast knowledge made us understand this project and its manifestations in great depths and helped us to complete the project successfully.

We would also like to acknowledge with much appreciation the role of the staff of Computer Department, especially the Laboratory staff, who gave the permission to use the labs when needed and the necessary material to complete the project. We would like to express our gratitude and appreciate the guidance given by other supervisors and project guides, their comments and tips helped us in improving our presentation skills. Although there may be many who remain unacknowledged in this humble note of appreciation but there are none who remain unappreciated.

## REFERENCES

**[1].** Yinyeh, M. O., & Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering.

**[2].** Prasad, H. K., Halderman, A. J., & Gonggrijp, R. (Oct. 2010). Security Analysis of India's Electronic Voting Machines. Proc. 17th ACM Conference on Computer and Communications Security (CCS '10).

**[3].** Frances Zelazny proposed the UIDAI, Biometrics Design Standards for UID Applications, 2009.

**[4].** Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan Vol-3 Issue-2 2017 IJARIIE-ISSN(O)-2395-4396 4252 www.ijariie.com 2145.

**[5].** Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013 .

**[6].** K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan , "highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May 2013.

**[7].** Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O. Hajari," A Remotely Secure E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 13 - Mar 2.

**[8].** Introduction to Computer Security, by Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2005.

**[9].** C. Neuman, T. Yu, S. Hartman, K. Raeburn, The Kerberos Network Authentication System (RFC4120), July 2005.

**[10].** K. Raeburn, Advanced Encryption Standard (AES) Encryption for Kerberos 5 (RFC3962), February 2005.