OVERCOMING TRADITIONAL VOTING ISSUES USING BLOCKCHAIN TECHNOLOGY

Piyush Mahadik , Uma Jain, Kunal Kharat, Suyash Kumbhar,

Final Year Student, Dept. Of Computer Engineering, Progressive Education Society's Modern College of Engineering, Pune, Maharashtra, India

Prof. Jayaprabha Kanase

Professor, Dept. Of Computer Engineering, Progressive Education Society's Modern College of Engineering, Pune, Maharashtra, India

---

Abstract - *Blockchain offers new opportunities to develop various new types of digital services. While more technologies are being explored, it focuses more on technical and legal issues rather than taking advantage of this novel opportunity and creating more advanced digital resources. We will use Blockchain open-source technology to propose a new electronic voting system that can be used in local or national elections. In a democratic country like India, voting plays a key role in the election of government officials and reflects our vision of how a ruling party should be built. Time to time, research was conducted to deal with the complexity of the central voting system so that it would be anonymous, reliable and secure while preventing any form of fraud. Even with the use of electronic voting, we have to deal with known security issues and fraud. Currently, various studies are being conducted to create a safe and reliable voting system while addressing issues of anonymity and security. We can use the Blockchain Technology and the decentralized system it provides to make the voting process easier, secure and anonymous in the public domain. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters and the public trust of their governments.*

Key Words*: *voting, online voting, blockchain, cryptography, election, hashing, ethereum

1.INTRODUCTION

Voting has long been considered a major way for people to share their views on controversial issues and debates. The current system provides anonymity to voters but is not considered transparent. People are expected to trust the results announced by the government when it comes to elections. There are many frauds involved in voting such as vote-rigging, booth capturing and voter fraud. The standard E-Voting systems are currently based on a well-known client server architecture: The server and voting data are governed by a trusted third party that is responsible for the ownership and integrity of the votes. Unfortunately, voting relies heavily on the credibility of the electoral authorities. In recent decades, a number of allegations have been leveled against the electoral process. In this paper we propose an online voting platform based on Blockchain technology aimed at addressing concerns raised by traditional E voting systems. The program introduces a new way of verifying and verifying eligible voters. Considering all the problems associated with the current traditional election system such as *vote tampering, standing in long lines to cast votes, booth capturing etc.* We are focused on eradicating such problems and bringing about transparency, authentication in our voting procedure. Therefore, replacing EVM based voting system with blockchain technology will have the following features:

1. Remotely accessible
2. Strong data integrity.
3. Decentralized control and validation by means of consensus mechanisms.
4. Transparent runtime environment.

2. MOTIVATION

1. To learn about different types of security issues and threats on blockchain technology.
2. To learn about preventive measures for the attacks.
3. To use the concept of blockchain to provide secure e-voting
4. To provide a secure voting environment and show that a reliable voting scheme is possible using blockchain.
5. To learn and discuss various new ideas and technologies to conduct online elections

3. OBJECTIVES

1. To propose a secure model for online election using Blockchain Technology
2. To satisfy the privacy and security requirements of electronic voting
3. To ensure that the election system should not enable coerced voting
4. To discuss theoretical structure of the proposed system with its limitations

4. LITERATURE SURVEY

Paper[1] ***Mohamed Ibrahim, Kajan Ravindran, Hyon Lee, Omair Farooqui, Qusay H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint***

Authentication", 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)

The design and development of a voting system that provides its own blockchain, running on a decentralized network of nodes, to maintain vote integrity and distinguish between registered and unregistered voters

Paper[2] ***Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access (Volume: 7)***

In this paper we were introduced to the concept of block creation and block sealing. It helps in making the blockchain adjustable to meet the needs of the polling process.

Paper[3] ***David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb, "Decentralized Voting Platform Based on Ethereum Blockchain", 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)***

To validate the proposed system various technologies are used. E.g. Solidity, NodeJS: Web3js HTML5

Paper[4] ***Giang-Truong Nguyen, Kyungae Kim, "A survey about Consensus Algorithm used in Blockchain", J Inf Process Syst, Vol.14, No.1, February 2018***

This paper explores a detailed qualitative and quantitative working of all the consensus algorithms used in blockchain right now.

5. PROPOSED SYSTEM

Our e-Voting solution will include four main requirements that can be illustrated as shown below:

1. Authentication: Only people already registered to the system can cast a vote. Our system will verify the user before casting the vote. Registration requires verification of certain documents and information as per the use case and application model of the system. We use a previously defined database to carry with the registration process of authenticating the user. Therefore, the system will be able to verify voter identities against the previously verified database, and then let the user vote only once.

2. Anonymity: The e-Voting system should allow prevention of voter identities and the casted vote. The voter and his casted voted must remain anonymous at all times during and after the election.

3. Accuracy: Votes must be accurate; every vote should be wholly counted, and can't be duplicated, changed or removed.

4. Verifiability: The system should be able to verify all the votes casted and make sure that all the votes are counted correctly.

5.1 The Blockchain:

The first transaction added to the block representing the candidate will be recorded as a special transaction. When this transaction is created it will include the candidate's name and with every vote for that specific candidate placed on top of it thus forming a chain for the respective candidate. Every time a person votes the transaction gets recorded and the Blockchain will be further updated increasing the tally of votes for the candidate.

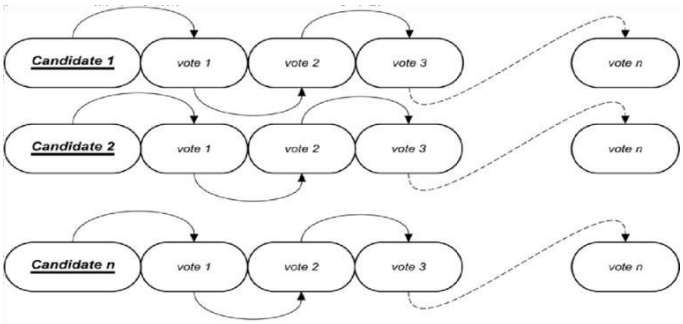


Figure 1: A Simple Representation of the Blockchain Structure of each Candidate

To ensure the security of the system, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out the error block since all blocks are connected and linked to each other. The Blockchain is decentralized and cannot be corrupted; thus providing us with the much needed security aspect for hosting online elections. The Blockchain is where the actual votes are stored. The user's vote gets sent to one of the nodes, and the node then adds the casted vote to the Blockchain. The voting system will have a single node in each given district to ensure the system is decentralized and safe from one single control of authority.

5.2 Representation of the e-voting system

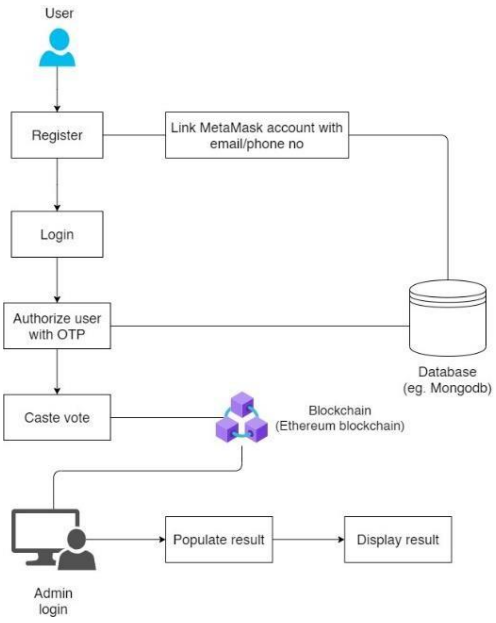


Figure 2: Simplified Representation of e-Voting System

(1) Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-Voting system will use his unique identity number, which will be verified through the previously provided database of unique identity numbers given by the local authorities. The system will check all information and, if matched with a valid voter, the user will be further authorized to cast a vote.

(2) Casting a vote: Voters will have to choose to either vote for one of the candidates from the given list of candidates. Casting the vote will be done through our interface.

(3) Encrypting votes: After the user casts his vote, the system will generate an input that contains the voter identification number as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output after encryption will be unique as well. The encrypted information will be recorded further in the block header of each vote cast. The information related to each vote by the user will be encrypted using SHA-256 hashing algorithm, which is a one-way hash function which is one-way and has no known way to reverse it. This way of hashing votes and storing it in the blockchain makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved once the formation of block takes place.

(4) Adding the vote to the Blockchain: After a block is created, depending on the candidate selected, the information is recorded in the respective block and then added to the chain of the block thus updating the Blockchain for the candidate. Each block gets linked to the previously cast vote to increase the number of blocks associated with the constructed blockchain of a candidate.

5. System Design

5.1 Software Requirements

React	17.0.2
NodeJs	v16.13.0
Firebase	v8.8
Ganache	6.12.2
Truffle Suite	v8.9.4
Metamask	v10.8.0
Vscode	v1.63.2

5.2 System Architecture

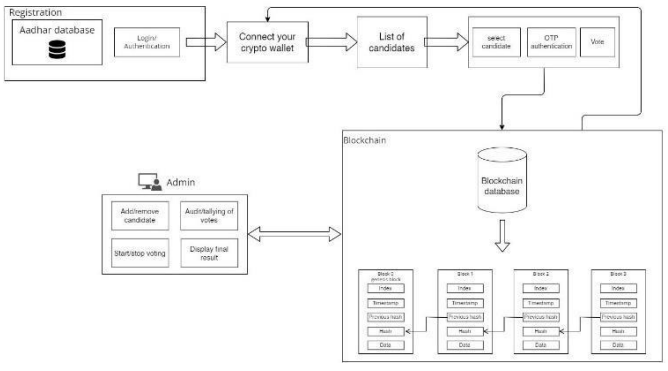


Figure 3: Architectural Block Diagram

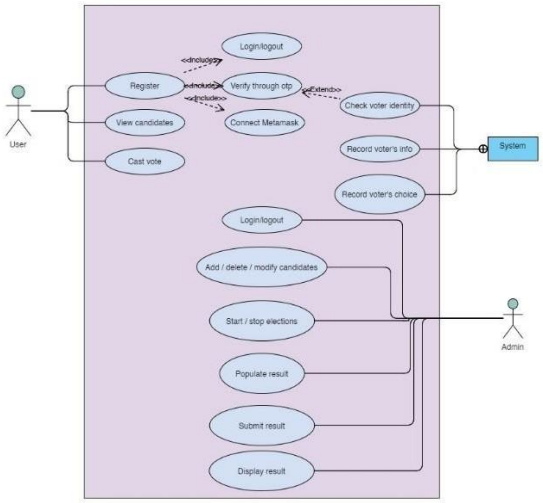


Figure 4: Use-Case Diagram

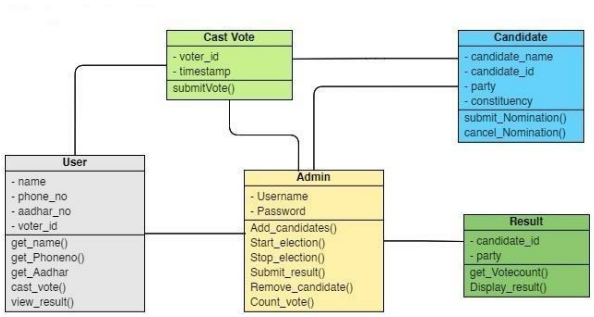
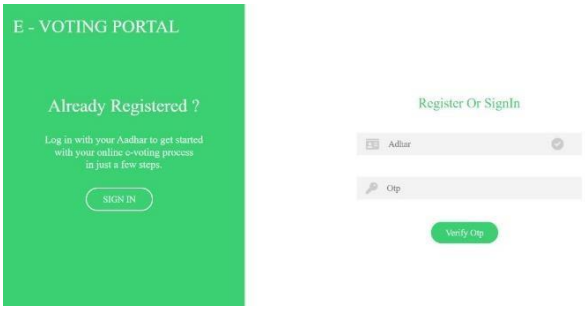


Figure 5: Class Diagram

5.3 Limitations

We assume that voters will use a secure device to cast their vote. Even while our system is secure, hackers have the ability to cast or alter a vote by initiating attacks or using malicious software already installed on the voter's device to rig the elections. One of the drawbacks of our proposed system is the inability to change a vote in case of a user mistake. The user will be able to cast its vote only once. There may be some technical glitches involved which may lead to some inconveniences in the voting process.

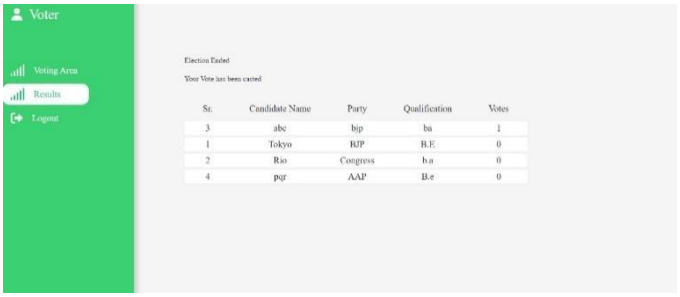
6. Result



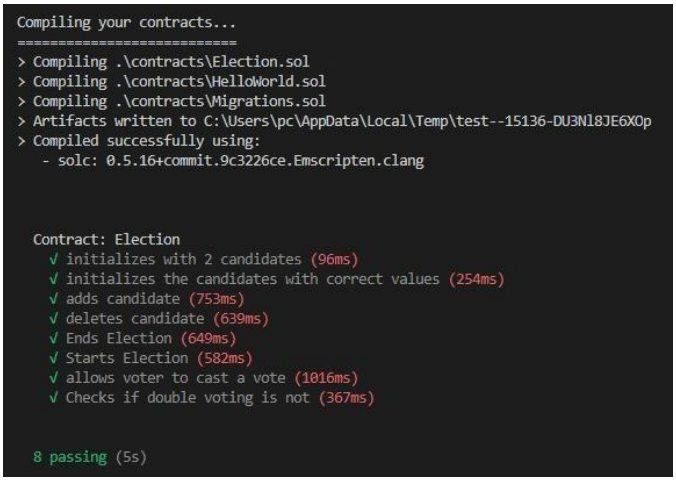
This is the portal where user can register himself using his unique identification which will be his adhar number in this

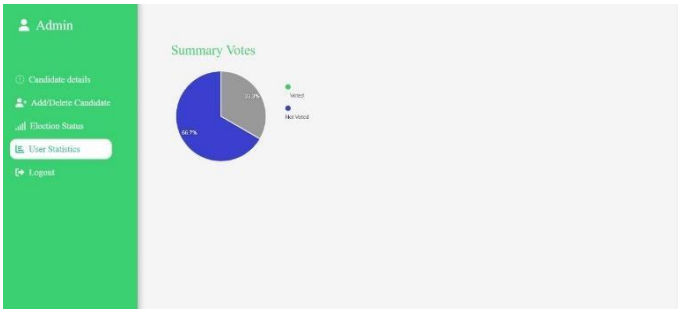
case, he will be then verified using OTP to check if he is a registered user in the database provided for list of officially registered voters, once verified he then will progress towards the voting area.

This is the voting area where the user will be teleported to his list of candidature where he can choose to vote for any one candidate as per his choice. Only a single vote is allowed which will later be stored in blockchain through encryption and hashing algorithms.



After the voting process, results will be announced





7. CONCLUSION

We have proposed an electronic voting system for elections through digital means based on the Blockchain technology. The system is decentralized and does not rely on trust of a single authority. Any registered voter will have the ability to vote online using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to edit or corrupt it making sure there is no rigging of elections involved as seen in the traditional voting system. The proposed system introduces a new way of voting, overcoming the problems faced in traditional voting system, paving a way towards the vision of digital education and use of upcoming technology to better everyone's lives.

ACKNOWLEDGEMENT

We would like to express our gratitude towards our college, "*Progressive Education Society's Modern College of Engineering"* and our college staff for constantly providing inputs and help whenever necessary. Our project guide and our project Co-Ordinator have been an immense support for our cause and project, providing us with much needed inputs and constant help whenever required. We would also like to thank all the professors around us for shaping our minds and setting our vision, all the teachers and professors who were working in the background to provide us the knowledge required to execute this project. We would also like to thank all our classmates for helping us giving valuable feedback, the college support staffs for providing us with all the required resources. We express our sincere gratitude for various industry experts who constantly checked our progress and provided us with suitable suggestions and changes. Lastly, we would like to appreciate the constant support of our friends and family.

REFERENCES

1. Mohamed Ibrahim, Kajan Ravindran, Hyon Lee, Omair Farooqui Qusay H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication", 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)
2. David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb, "Decentralized Voting Platform Based on Ethereum Blockchain", 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)
3. Giang-Truong Nguyen, Kyungae Kim, "A survey about Consensus Algorithm used in Blockchain", J Inf Process Syst, Vol.14, No.1, February 2018
4. Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access (Volume:7)
5. T. Dimitriou, "Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting," Computer Networks, vol. 174, p. 107234, Jun.2020
6. T. K. Sharma, "Top Countries That Conducted Elections On The Blockchain," Blockchain Certifications, 15-0ct-2019. [Online]. Available: https://www.blockchain-council.org/blockchain/top-countries-that-conducted-elections-on-the-blockchain/. [Accessed: 13-Feb-2021]
7. E. F. Kfoury and D. J. Khoury, "Secure end-to-end voip system based on ethereum blockchain," Journal of Communications, vol. 13, no. 8, pp. 450–455, 2018.

8. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.
9. A. Shah, N. Sodhia, S. Saha, S. Banerjee, and M. Chavan, "Blockchain Enabled Online-Voting System," ITM Web of Conferences, vol. 32, p. 03018, Jan. 2020.
10. Ali Kaan Koç, Emre Yavuz, Towards Secure E-Voting Using Ethereum Blockchain, 1st ed, vol 1, 2018 IEEE.
11. P. Tarasov and H. Tewari, "The future of e-voting." IADIS International Journal on Computer Science & Information Systems, vol. 12, no. 2, 2017.