



Voting System Based on Blockchain

*Ganesh B. Regulwar^{#1}, N.Sai Shashank^{#2}, Nikhila Kathirisetty^{#3}, K.Jaya Krishna^{#4}, Farhana Begum^{#5}, S.Sai Akhil^{#6}

^{#1, 2, 4, 6} Information Technology Department, ^{#3, 5} CSE (Data science) Department, Vardhaman College of Engineering Shamshabad, Hyderabad, Telangana, India

Abstract— Voting is a vital event for any country and most importantly for a democratic country. Unfortunately the end results of such existing voting systems are being tampered by events such as election manipulation, voter fraud or vote rigging etc. It is the need of the hour to address such issues and voting system which is both secure and immutable, to achieve these properties, the concept of blockchain is incorporated into the existing voting system in-order to make it secure, free from tampering and also reduce the cost involved in voting. This is made possible by developing a web application which acts as an user interface so that the voter can cast their vote, ganache tool has been subsumed into the project to mimic a local block chain network and metamask wallet is made use of for authentication and validation purposes, this process enables hassle free election process along with an error free result.

Keywords— *Immutable, blockchain, ganache, metamask, truffle*

I. INTRODUCTION

Generally, in the current day scenario voting is conducted by a central regulatory body who is responsible for the smooth and hassle free conduction of the election process. Unlike the traditional system, blockchain offers the feature to exploit the principles of decentralization as it has only a series of blocks involved with each block containing the hash value of the previous block. It is because of this the blockchain technology is immutable [1] in nature since all the blocks are connected to the previous blocks. This peculiar feature of immutability of this particular technology has resulted in various use cases since a technology that is immutable is highly secure and many use cases have branched out of this one of which is the

electoral system. In the current day scenario Electronic voting machines are used across the country to conduct elections which is a very outdated and an orthodox method of conducting elections which is one of the most crucial event. There is an urge for new technologies to take over these electronic voting machines (E.V.M.). [2]It offers lower security and integrity to the voting system and there are always scenes of tampering these machines as they are physical entities and like all physical machines these can be tampered which might affect the fair and transparent conduction of elections. To overcome such drawbacks there is a huge vacuum for new technology to take over, blockchain is one such it has a ledger based technology which incorporates security by using the concepts of cryptographic hashing and also the most vital aspect being its is immutable i.e. it is not possible to alter or update any entries that are made into the blockchain. The main reasons accounting for the growing need for a dependable voting system are as follows:

1. There are lots of security breaches leading to tampering of votes and data leaks.
2. Time consuming process because lot of paper work involved.
3. Physically challenging for aged and disabled individuals.
4. The cost incurred in conducting elections is high.
5. It is not transparent.
6. It takes lot of time to count the votes physically and there a scope for human error eventually resulting in delayed results and in certain cases faulty results.

All the above stated reasons account for a novel voting system which is tamper proof, makes the process of voting easy and comfortable and address the draw- backs of the current voting systems.

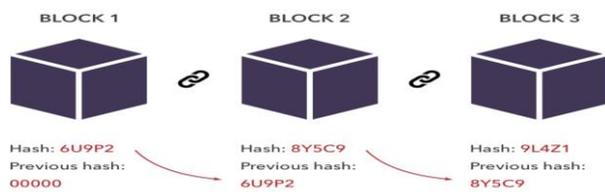


Figure 1. [10]representation of blocks in blockchain

II. LITERATURE SURVEY

In this literature [4] Blockchain employed as a service is being evaluated to implement electronic ballot system. A system that utilizes "permissioned blockchain" for an e-voting system based on blockchain to alter liquid democracy is being proposed along with research on suitable blockchain frameworks to construct this blockchain based e-voting system. [5]The research paper proposes a decentralized trust less e-voting system based on the blockchain algorithm. The voter does not need to rely on the election administrator as the trust is separated to all voters and the computation is dependent on the decentralized blockchain. Due to this the tally result will not be altered even if the election administrator is malicious as it uses a private public key pair encryption without third party. Instead of using the bit coin network which requires proof of work this works on the Ethereum network to record the voting result from every place of election. [6]In this literature Authentication is being incorporated in this model which is an android application with enhanced security features along with authorization features. A unique identification key and fingerprint is used for authentication and authorization respectively. A one-time password is also sent for voter verification. This project implements security by a 128-bit AES encryption algorithm and SHA-256 with blockchain technology. Atomicity and integrity are maintained as a blockchain, in which votes are casted in the form of a transaction, keeps track of the tallies of votes. [7]This literature uses the blockchain to address problems of voter access and voter fraud. The method deploys an encrypted key (RSA private key) and personal verification such as fingerprint biometric verification to authenticate voters. The voter then casts the vote which will be encrypted and added to the blockchain in the server. A few algorithms used in this project are Merkle root, SHA3, RSA and blockchain voting. SHA3 is used for hashing. [8]This literature puts forth the idea where they suggested a voting application to conduct election process in the United Arab Emirates (UAE).It provides an overview of all

the advantages of using the blockchain technology like minimizing the costs incurred at the same time also ensuring integrity. It also prevents fake votes by implementing authentication features to the voting system; this also makes the process paperless. [9]his research work suggests how the process of elections can be made transparent using the blockchain technology it clearly provides an overview of how the attack 51 can clearly be avoided by preventing any such miner with such high hash rates from mining or employing miners solely for the purpose of mining during the election process .

III. PROPOSED FRAMEWORK

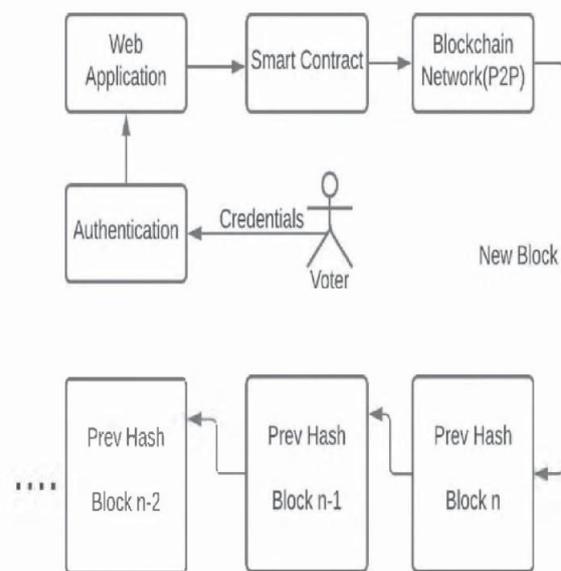


Figure 2. General flowchart of the proposed system

Objectives

The following considerations are taken care of to attain the objectives:

1. Each voter should cast their votes only once.
2. Each voter should be associated with an address and a private key.
3. The votes need to be in a verifiable format and a token of the vote casted need to be generated, not only this they also need to be tamper proof.
4. The casted votes should be recorded to prevent fraud and generate immediate results.

The following are the objectives of the designed system:

Privacy - Keeping an individual's vote secret. The system makes use of cryptographic concepts which tend to keep the identity of the voter a secret by storing the hash values thereby ensuring the privacy of the voter.

Verifiability-Each and every vote that is casted is stored as a transaction and serves as a proof that can be verified in case of any discrepancies regarding the casted vote in the future.

Transparent-The system designed is in such a way that all the details are available for use by the public and conducting authorities in order to prevent any kind of unjustful activities.

Faster -The system should be fast in way that the count of votes of each candidate is updated at regular intervals and a record is kept in order to prevent the tedious process of counting the votes which might result in human errors.

Ganache

Ganache is employed to kindle a private Ethereum blockchain that you'll use to run tests, execute commands, and examine state whereas dominant however the chain operates. For implementing this projected work associate degree Ethereum blockchain network is employed. It is a decentralized application which is used to mimic the actual working of the ether test network so that develop new applications on such test networks without having to spend actual ethers as it will turn out to be a very costly affair. It since, it is based on ethereum is makes use of ether (ETH) which are fake. It is based on the accord algorithm rule and uses the concept of proof of work. It has a series of blocks which has information that is being encrypted by using cryptographic hashing techniques and each block is linked to its previous and next blocks in order to ensure that the system is immutable any change made in one of the block reflect in all the others as they are enchaind in a series as depicted in Fig. 3.

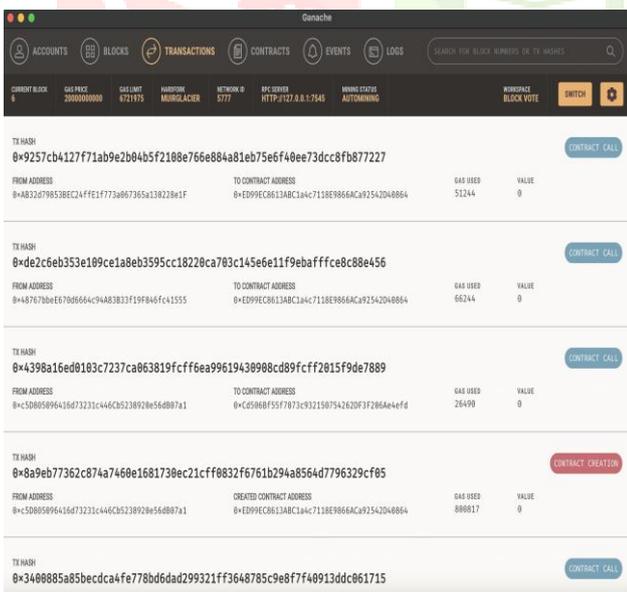


Figure 3. ganache framework

Truffle Framework

Truffle is employed to take care of managing your con- tract artifacts thus you do not have to be compelled to do so. Includes support for custom deployments, library linking and sophisticated Ethereum applica- tions. Here the tendency is to use truffle framework to deploy the smart contracts as shown in Fig. 4 written for the method of option.

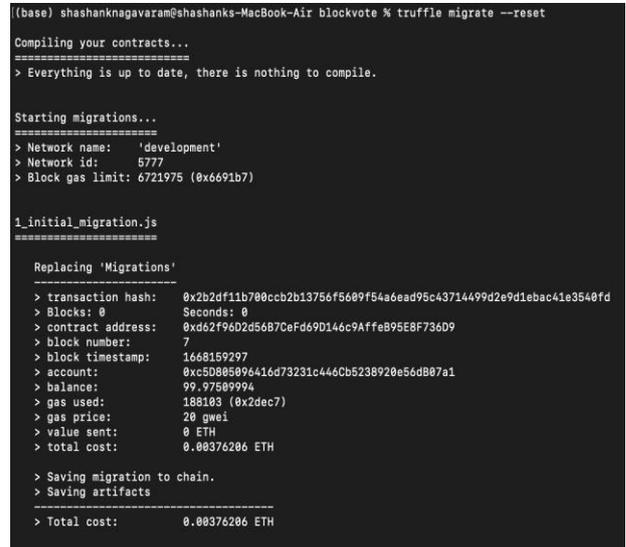


Figure 4. truffle contract deployment

Metamask

It is a wallet which is used to store our crypto currency. Here the web browser extension version of the metamask is used, first one need to connect this metamask wallet to the web application in order to cast our vote. Once, vote is casted for a candidate a token is generated on the metamask wallet which consists of the information regarding the gas fees and etc. for casting our vote. On confirming the vote is casted to the candidate chosen. This token serves as a proof that a voter has casted their vote

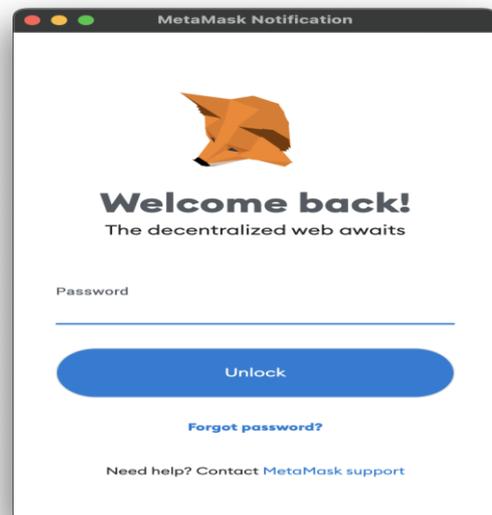


Figure 5. Metamask login page

Web Application

Finally web application is developed as a part using the scripting languages javascript, html and also css is used to add interactivity to the web application. This is the section which acts as the user interface for the voters and they can select the candidate from the dropdown menu and vote for their desired candidate. Once voted, the casted vote is recorded and written into the blockchain and the candidate cannot vote any further.

IV. RESULT

The end product is a web-application developed on the basis of the [5]blockchain. After the vote is casted voter is redirected to the metamask wallet from where they authorise their vote by clicking on the confirm button as shown in Fig.6, 7. Once, the voter confirms the transaction then the transaction is written into the local blockchain thereby, maintaining a record for future reference in case of any discrepancies. on confirming the voter is redirected to the web application where a pop up message shows that they have already voted as depicted in Fig. 8 and they can't vote any further.

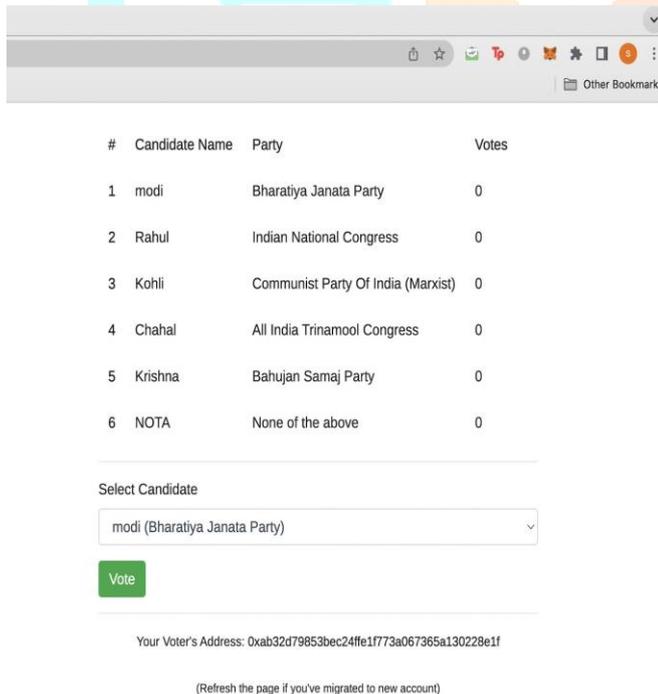
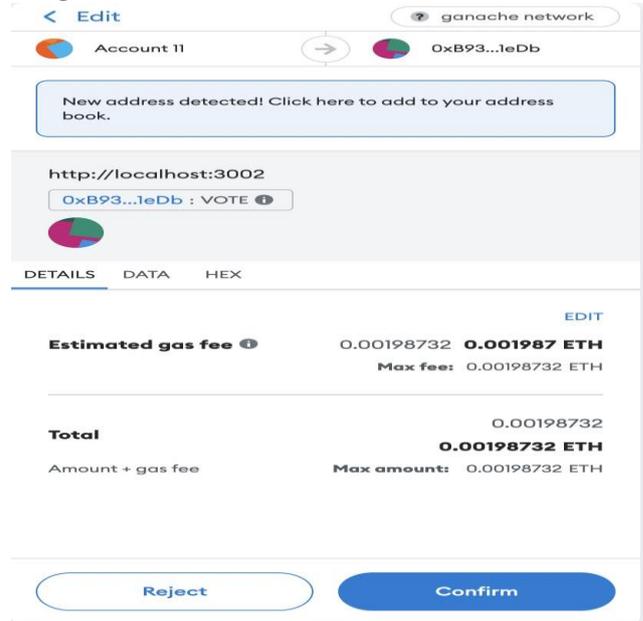


Figure 6. user-interface to cast vote

Figure 7. Transaction on metamask



wallet

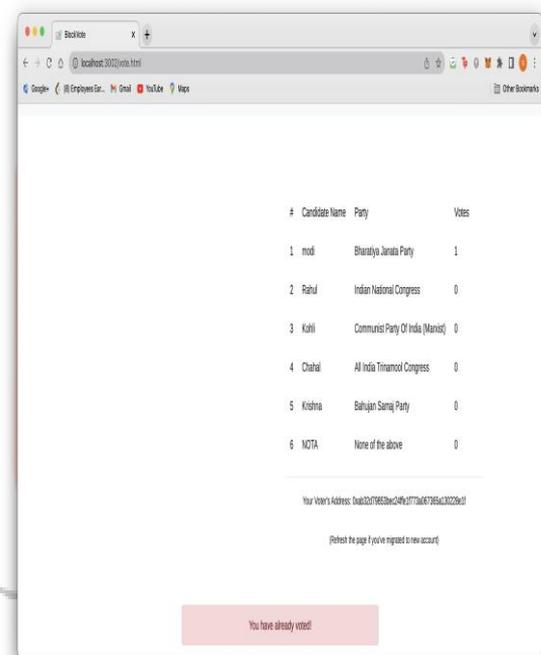


Figure 8. Completion of voting

V. CONCLUSION

Through this paper we put forth the idea of conducting elections on a voting system that is developed on the grounds of blockchain technology in order to ensure a safe and secure set-up for smooth and efficient conduction of elections, apart from these one of the key motto of this research work is to guarantee a sense of privacy to the voter. Although this topic might serve as a point of disagreement and controversy among several political and scientific circles, it provides a ray of light to include futuristic technologies not only in everyday activities but also in such crucial events. It also provides for the cost cutting aspect in conducting elections which

might save some economy in the event when country is going through a rough patch financially or facing a financial crisis. The existing traditional e-voting systems developed on the grounds of technologies such as php, sql, dbms in such systems one can insert, update and delete the casted votes. On the contrary, since the concept of blockchain is incorporated it acts as an immutable ledger i.e one cannot update or delete records but only insert the records.

VI. FUTURESCOPE

As discussed in like every coin has a second side there are also certain setbacks of the system that is developed by exploiting the principles of blockchain. Although it has several benefits such as security, privacy of voters, transparency and so on but the major setback is that verification is present on an account level and it would not be possible to verify on a private level and in-person verification would require a whole new system. [11] Although Blockchain Technology has a wide spectrum of applications, in the current day scenario it is just in the beginning phase and it needs a lot of efforts and analysis to reach its full potential.

REFERENCES

- [1] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, 36, pp.55- 81, 2019.
- [2] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", in ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom
- [3] Bhabendu Kumar Mohanta et al, "Blockchain Technology: A survey on Applications and Security Privacy Challenges", *Internet of Things*, pp1- 20, 2019.
- [4] "Blockchain technology based e-voting system." Prof. Anita A. Lahane, Junaid Patel, Talif Pathan and Prathmesh Potdar *ITM Web of Conferences* 32, 03001 (2020)
- [5] Blockchain Based E-Voting System Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Anshu Ghodeswar, Prashant Parde "Blockchain Based E-Voting System" *International Journal of Scientific Research in Science and Technology* May-June-2021
- [6] "Blockchain Enabled Online-Voting System" Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, Madhuri Chavan *ITM Web of Conferences* 32, 03018 (2020)
- [7] "Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root" S. Aruna, M. Maheswari and A. Saranya *IOP Conference Series: Materials Science and Engineering* (2020)
- [8] N. B. Al Barghuthi et al., "An Analytical View on Political Voting System using Blockchain Technology - UAE Case Study," *2019 Sixth HCT Information Technology Trends (ITT)*, 2019, pp. 132-137, doi: 10.1109/ITT48889.2019.9075074.
- [9] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in *IEEE Access*, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.
- [10] Anupong Wongchai, Surendra Kumar Shukla, Mohammed Altaf Ahmed, Ulaganathan Sakthi, Mukta Jagdish, Ravi kumar, *Artificial intelligence - enabled soft sensor and internet of things for sustainable agriculture using ensemble deep learning architecture*, *Computers and Electrical Engineering*, Volume 102, 2022, 108128, ISSN 0045-7906
- [11] Mrunalee Dhone, Ganesh Regulwar (June 2020) "Credit Card Fraud Detection by Applying Deep Learning", Published in *International Research Journal of Engineering and Technology (IRJET)*, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume 7, Issue 6 pp.1491-1494, June 2020.
- [12] Gitanjali. A. Kadlag, Ganesh Regulwar (May 2020) "Detection and prevention of data modification attack based on MD5 algorithm", Published in *International Research Journal of Engineering and Technology (IRJET)*, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume 7, Issue 5 pp.6912-6914, May 2020.
- [13] A.S. Nagdive, G.B. Regulwar (March 2019) "Web Server log Analysis for Unstructured data Using Apache Flume and Pig", Published in *International Journal of Computer Sciences and Engineering (IJCSE)*, E-ISSN: 2347-2693, Volume 7, Issue 3 pp.228-233, March 2019.