IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Online Voting System using Blockchain Technology

Dr. Nandkishor Karlekar[1], Vaibhav Kumbhar[2], Subodh Mohite[3], Pranav Kadam[4], Hareram Mane[5]
Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
Mahatma Gandhi College of Engineering and Technology, Navi Mumbai, Maharashtra, India

Abstract: *A widespread mistrust towards the traditional voting system has made democratic voting in any country very critical. People have seen their fundamental rights being violated. Other digital voting systems have been challenged due to a lack of transparency. Most voting systems are not transparent enough; this makes it very difficult for the government to gain voters' trust. The reason behind the failure of the traditional and current digital voting system is that it can be easily exploited. The primary objective is to resolve problems of the traditional and digital voting system, which include any kind of mishap or injustice during the process of voting. Blockchain technology can be used in the voting system to have a fair election and reduce injustice. The physical voting systems have many flaws in it as well as the digital voting systems are not perfect enough to be implemented on large scale.Furthermore,the methodology for carrying out blockchain transactions during the process of voting has been elaboratedusing Blockchain Finally, the performance evaluation of the proposed system shows that the system can beimplemented in a large-scale population*

Keywords: E-polling, voting system, blockchain application, blockchain voting, E-voting, electoral system, blockchain, cryptographic hash, secure voting

I. INTRODUCTION

Blockchain can reduce a lot of efforts and resources invested in polling stations, specifying the areas, appointing staff, and preventing security risks at polling stations. Holding a digital election through blockchain not only saves money but also reduces the risk of inequity in the voting process. Modern technologies such as blockchain technology are very secure and beneficial if used carefully. It can make the voting system more transparent, reliable, and also enhance traceability of transactions.

In a traditional digital voting system, a voting machine has been used which is connected to a centralized database. This machine can be tampered with by a person who has physical access to it. It may cause single point of failure in the whole network of the voting system; on the other hand, an immutable blockchain would not be affected by an individual saboteur in the network. In a blockchain, the data is being stored in a decentralized manner, which is constantly verified if the records are accurate. Therefore, in case of a malicious attack on a node, only that node would be affected and peer to peer network still provide all services. It makes blockchain technology a threat proof and reliable system to be used as a private ledger in the voting system. Blockchain has offered a level of security and trust more than the previously used technologies. The resources can be saved by hiring less staff, security forces, and arranging polling stations for a traditional voting system can be given to the miners.

II. PROBLEM STATEMENT

The percentage of polling on the day of elections is not satisfactory as majority of the people are not coming to vote and thinks is just as a wastage of time. The manual voting system takes long time as there is a lot of paper work first and then human effort is also there for counting of the votes. Manual voting consumes almost 4-6 hrs. (approx.) of every voter which is surely a headache.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

The voting will be done online such that there is no need to come at the place on the time of elections and the people can vote from the home or from any other place. A key will be provided to every person, so that on the time of elections they can easily login on the election link and can cast his/her vote.

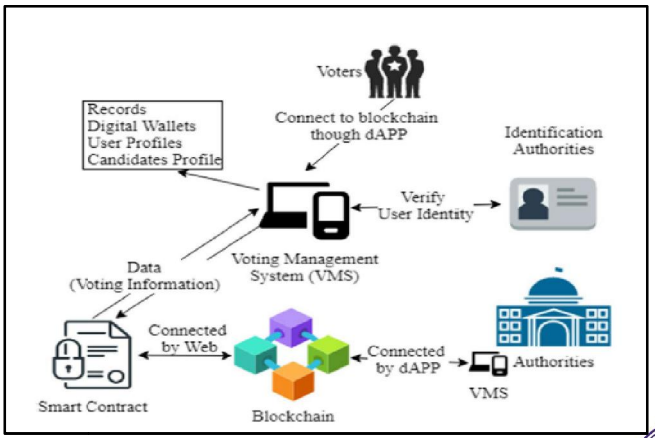
III. LITERATURE SURVEY

TABLE I

Title Name	Year	Publisher	Description
Blockchain-Based E-Voting System	2018	IEEE	This paper evaluates the use of blockchain as a service to implement an electronic voting (e-voting) system. The paper makes the following original contributions: (i) propose a blockchain-based e-voting system that uses "permissioned blockchain", and (ii) review of existing blockchain frameworks suited for constructing blockchain-based e-voting system.
Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract	2020	IEEE	Our objective is to design a Digital Voting architecture with the inclusion of a smart contract to reduce challenges generated during the adoption of blockchain with voting and provide authentication, transparency, anonymity, accuracy and autonomy, singularity, integrity, mobility. In our system, from the voters information a hash will be generated and stored in the chain. This will provide scalability and anonymity of voters as the information is stored in the blockchain as a hash.
E-Voting Systems using Blockchain	2020	IEEE	The blockchain network can be either a permission-less network like Bitcoin or Ethereum where anyone is allowed to interact with the network, or a permissioned network like Hyperledger Fabric, Hyperledger Sawtooth or Exonum where only known members are allowed to interact with the network. Another important issue to be addressed is the anonymity of the voter

IV. SYSTEM ARCHITECTURE

In Figure a high-level architecture of the proposed system has been presented. It shows how the main stakeholders; Voters, VMS, AA, and IA work together to perform certain voting tasks. All voters are connected to VMS directly through dAPP; it is either a mobile application or a web portal. The identification authority verifies voters registering in the system. Any voter who is verified and eligible to vote is allowed in the application to take part in voting. The process of the whole system includes certain parts; the first one is the user interface of the application, which also requires front-end security. It is critical because the user enters his credentials on that interface, so it should be secure and simple. The system provides full and fair access to every user during voting activity. It also provides traceability after casting of vote.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

The voter registers in the system by his credentials. VMS uses the ID details of voters and verifies them with online records of IA to register the voter in the system. The user receives a unique OTP to log in to the system. An OTP is generated each time the voter wants to login into VMS. All the detail of the voter is saved in VMS. After successfully registering in the system, One Voting Coin (VC) is added to the wallet of each voter. To prevent voters from voting twice, each voter is given only one VC.

V. WORK FLOW OF PROPOSED MODEL

The voter after completing the verification is registered into the Voting Management System. A single chain system is implemented on the blockchain. The national database of the country is also integrated with the system to keep the voter's voting integrity. For every vote, a transaction is being generated against the voter's National ID. The transaction is then mined by the minors and saved in the blockchain. When the voter casts the vote, his Vote Coin in his/her wallet is also being utilized. The voter cannot cast another vote after one vote coin is utilized. As the voter will sign-in through his/her credentials then the voter has been redirected to the election interface where all the candidates who are contesting in his constituency are shown to the voter. Upon the voter's request to cast vote, VMS verifies the voting status of the voter from the blockchain by checking all transactions hash that already exists against his/her computerized National ID. If a transaction hash is found against the voter's computerized National ID then VMS declined the request and logout the voter from the system. If a voter has not voted yet, the request is transferred to the miner to add the node. The voter selects the desired candidate and casts his vote. The transaction is monitored with the help of a transaction hash and carried out by the miner. The node is then added to the chain for balloting.

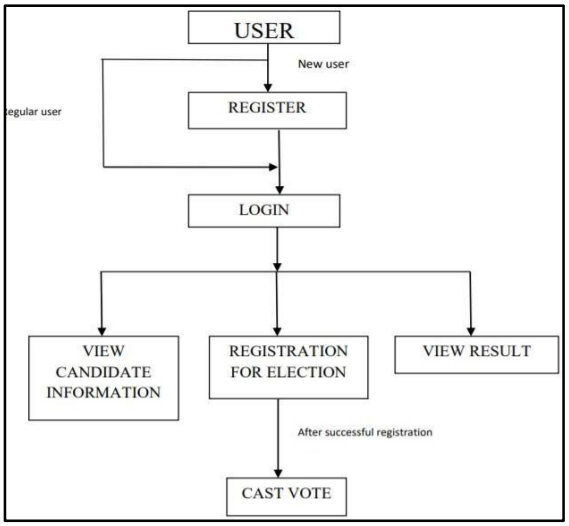


Fig.User flow diagram

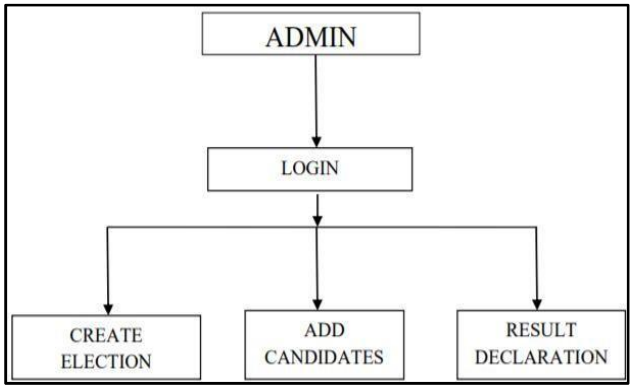


Fig. Admin flow diagram

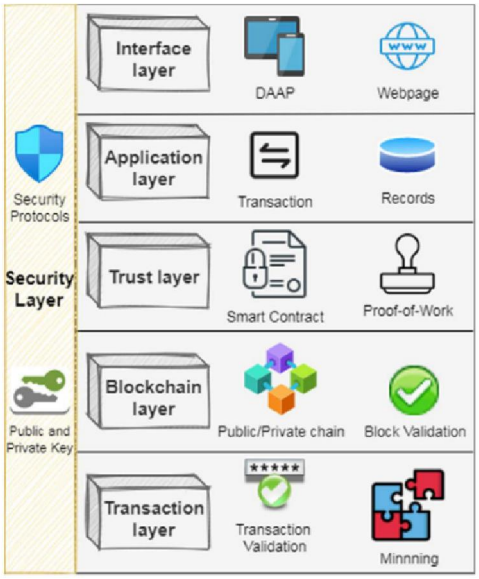
Voters must have access to any smartphone or web browser to take part in voting. The voter's interface would be provided in multi-languages to make it easy to use for all users. The proposed system can contain a large number of voters at thetime of voting. A decentralized blockchain system enables a voter to vote from any part of the world. A person can take part in voting from anywhere, even if he is in a foreign country, in this way his/her computerized National ID is verified from the national database so he can cast the vote. Voting transactions are sent to a pool from which miners analyze them and remove the malicious request by taking the consensus from the other nodes before adding it to the chain. The votes are fully secured using a cryptographic hash. Each vote cast adds a new block in the chain. System also make sure that only one vote can be cast by one user by using the vote coin. Even if due to some technical fault, the balance of the voting coin does not get updated, hence system ensures that no double votes have casted by a voter. By checking whether a transaction hash is generated against voter computerized National ID or not, if any node or request of a voter is malicious then miner automatically rejects it. When the transaction completes and a node is successfully added to Vote Chain, the voter of that particular voting transactionis noticed through an SMS to his registered phone-no an email. The voter has provided with a unique transaction hash by which he can verify his vote

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

through a web portal and upon successfully completion of transaction the vote has been counted in the whole voting activity. The voter wallet has then contained zero vote coins, when a voter successfully casts the vote.

VI. LAYERED STRUCTURE OF THE PROPOSED VMS

The proposed framework has been presented in a layered structure. System services have been bifurcated the process into five layers, it has the following layers presented as shown in figure. The interface layer contains all the dAAPs developed for voters and administration. These are the distribute APPs through which any stakeholder can connect to VMS. The goal of this layer is to provide an interface for interacting with the system. Application Layer provides a user verification system by involving external sources. It is the front-end interface of the whole voting system. It encapsulates the data of the voting system in online databases.



All the blockchain transactions are also handled in this layer. The user is verified by his/her National ID, that was eligible to take part in this voting activity. The Trust layer is the most important part of the whole framework. It ensures consensus is made correctly and the data is transferred securely through smart contracts. It verifies every new block added to the chain.The basic information related to the blockchain is stored in the blockchain layer; it keeps track of any faulty node in the chain to ensure the immutability of the chain. All the public and private keys, and transaction data are stored in this layer.

The transaction layer encompasses all the transactions that are made by using smart contracts between VMS and voters. Mining of all the transactions takes place in the transaction layer. The most critical layer is the security layer by which the blockchain is protected from any attack. Any attempt of attack is defended by using algorithms and basic rules that make it difficult for external entities to harm the chain. The security protocols are implemented on the entire chain. The private and public keys make data encrypted and secure throughout the system.

VII. IMPLEMENTATION DETAILS

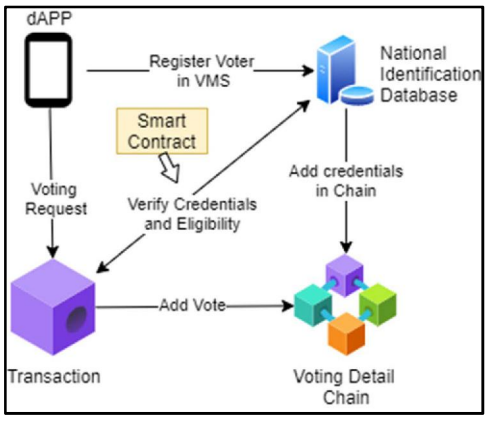
The process of voting is run by maintaining our system that is backed up by the blockchain. The hashes of transaction for every voter has stored on the chain and all the results of the election are also stored on the blockchain and from there the result of the election can be viewed on the resulting dashboard of the users. The system first verifies whether the voter is the country nationality holder and it also checks whether the voter has already voted or not if he still has a vote coin, the system allows him to cast vote. After verifying the voting details i.e voter identifier, vote, and timestamp was stored in the chain which saves vote details. The whole process is elaborated in figure.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

dAPP SETUP

Voting Management System consists of different components discussed in this section. It has a user interface for secure interaction of voters with the system, which also includes front-end security. A dAPP interface has been implemented front end of the VMS. The dAPP is a decentralized application based on blockchain technology. It runs on a P2P blockchain network. The user identification is critical because the user enters his/her credentials on that interface, so it should be tamper-free and simple. The system provides full fair access to every voter and provides traceability after casting the vote. The voter login the system by his/her credentials. System uses the ID details of the user and verify them with the Database to register the user in the system.

The user gets a unique OTP to log in to the system. The OTP has generated each time the voter login into VMS. The purpose of using the dAPP system is to ensure the reliability of VMS; as decentralization makes processing efficient at all nodes. If one node of the system during the voting system gets vulnerable, all the other nodes are not harmed. The node which gets vulnerable is reinstate by other nodes.



Election as a smart contract:

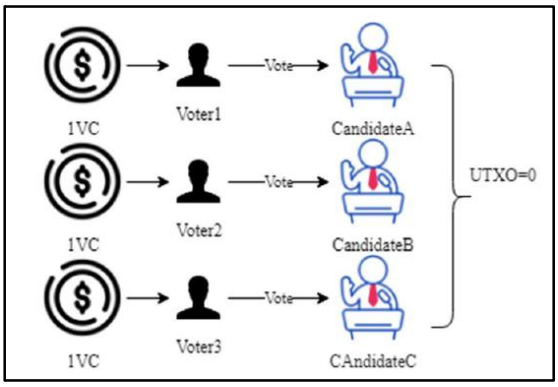
Smart contracts are providing a secure connection between the user and the network while executing a transaction in the chain. These are the rules that are implemented on the entire blockchain and cannot be neglected under any condition. All the nodes have to follow the smart contracts to save the vote in the system successfully.

The first smart contract is for user verification between IA and the VMS; it uses the Can-Cast-Vote function which checks the requirements of the system to make sure the specified voter can vote. After verification, it enters the voter details record for further use. The voter is being connected with a voting smart contract that specifies which candidates would be shown to him/her. If the consensus between the node and chain agrees then voting is allowed. The smart contact to cast vote in the system is defined in figure It checks the Vote Coin in the wallet of the voter, whether he/she has eligibility to cast vote or not. A function Cast vote is defined which takes voters' National ID and the wallet address as input and checks if the user voting coin is available. If the voter has a voting coin then the smart contract allows them to cast vote otherwise it has rejected the vote request.

TRANSACTIONS IN VMS (UTXO) :

This section explains the concept of Unspent Transaction Outputs (UTXO) in the proposed system. As discussed in Section IV part c, each voter is given one VC in his wallet at the time of registering. Voters can spend it only once while voting for candidates. Voting transactions in VMS are performed using the UTXO mechanism. In figurethere are several transactions by different voters to candidates. While performing each transaction 1VC is spent. Miner gets this VC as a reward. There is no transaction fee in the voting system as system keep the rights of all voters equal. Voter1 spends 1 VC to cast the vote for Candidate2. This transaction is recorded and forwarded to the memPool of transactions. From there, miners pick up multiple transactions and start to mine. Here the value of UTXO after each transaction is updated to zero, ensuring that a voter cannot vote again

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

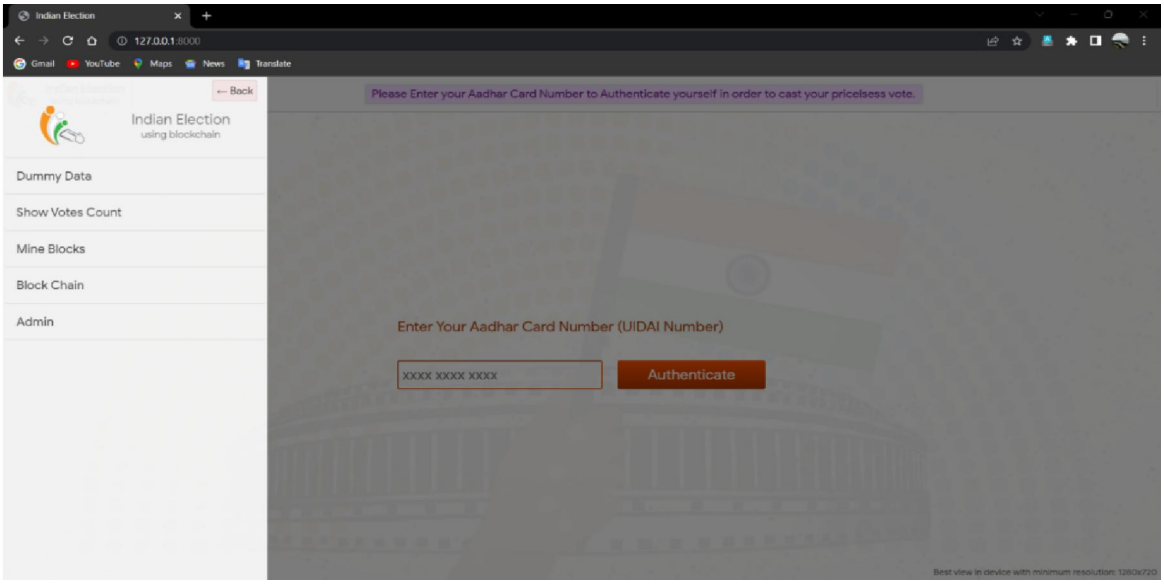


VIII. ALGORITHMS

- Algorithm 1:- Smart Contract: Casting Vote in VMS
- Algorithm 2: Smart contract: Registering in VMS.
- Algorithm 3: Chain security algorithm.
- Algorithm 4 : UTXO, Consensus Protocols, Cryptographic Hash.

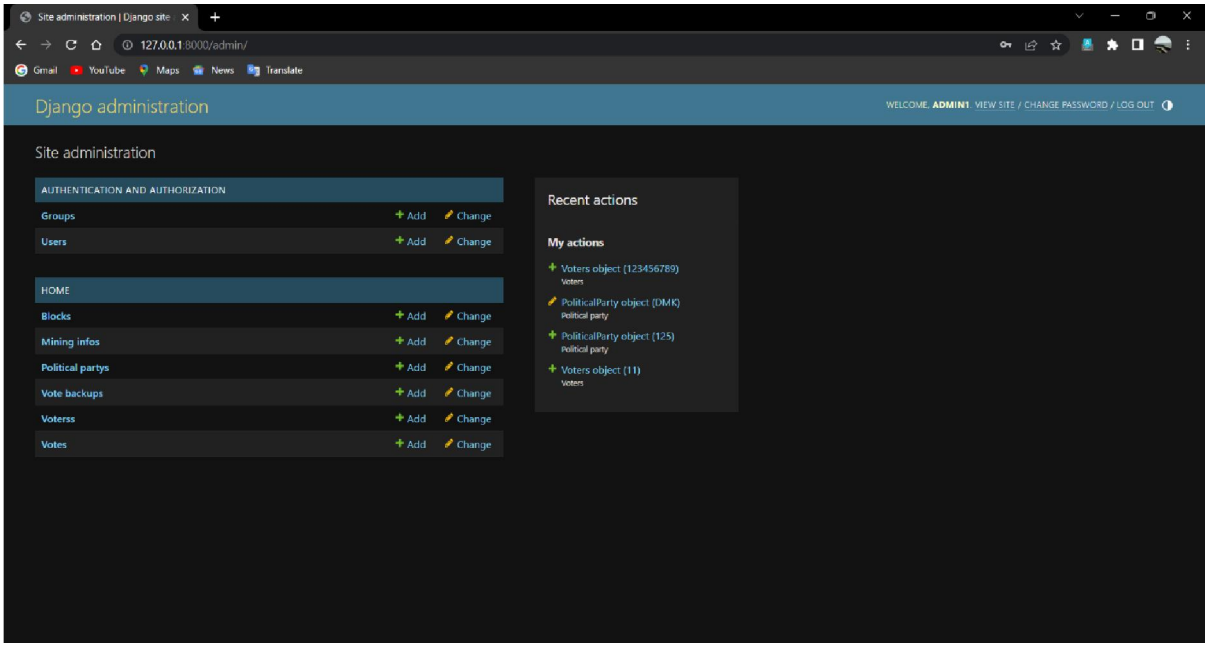
IX. OUTPUT

Home Page:

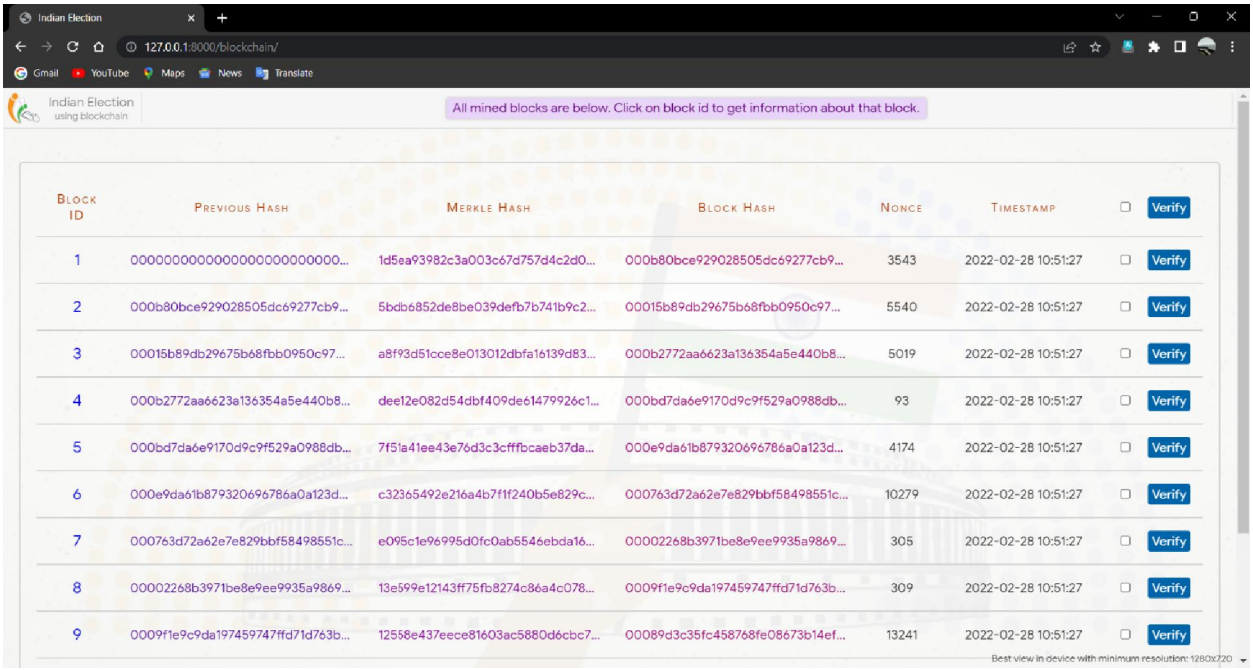


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Admin Page:

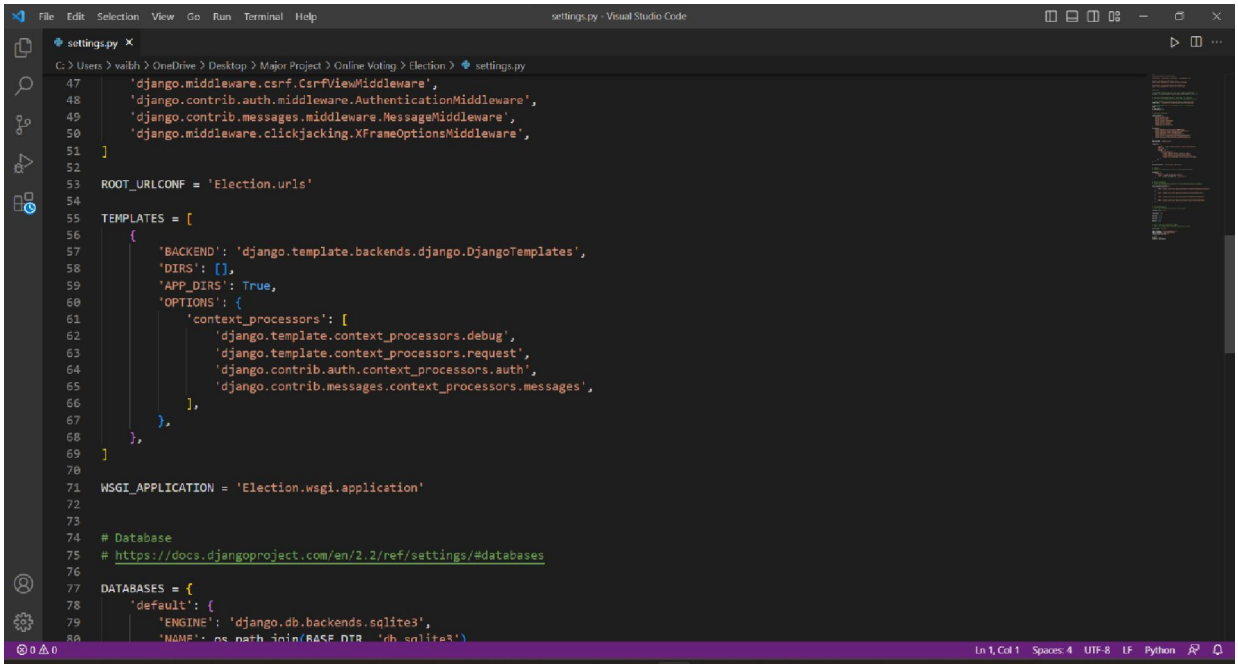


Mined Blocked Information:



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Backend Page:



X. CONCLUSION

The purpose of proposing a blockchain-based solution for the voting system was to build trust between government and voters to make-believe that their voting integrity is kept safe. The blockchain-based voting is also make the voting process transparent and trustworthy. The amount of money spent on voting activity in any country is very high for the traditional voting system, whereas the proposed solution for using the blockchain voting systems to make the voting process cheaper, faster and trustworthy. It helps to enhance people's relations with their democratic state, as they get a transparent system on which they can rely and trust. The framework elaborates on the feature, services and role of official authorities using blockchain in the voting system which is highly in need to improve the level of the electoral system and its reliability, traceability and trust. The verification of each vote makes it immutable. The use of hash assures the privacy of voters and the concept of public and private keys allows the authorities to control the process precisely. The traceability of the voting system assists in preventing hackers from modifying or viewing the voting information. It assures that one voter only votes one vote. The usability of this system performs well by using the more effective approach of implementing a flexible consensus algorithm to reduce extensive computing resources in the blockchain.

This transparent behaviour of the system tends to be promising for voters to rely and trust. The Chain Security Algorithm is also added, which automatically verifies the validity of the chain each time a new block is added to it. Smart Contracts play an important role to prevent any incomplete and malicious transactions in the blockchain voting system.

XI. ACKNOWLEDGEMENT

We would like to express our gratitude to the M.GM College of Engineering and Technology for providing us wit the necessary resources to conduct this research. We would also like to thank Dr. Nandkishor Karlekar for her guidance and support throughout the project. Additionally, we are grateful to project coordinator Prof. S.P. VidyaBharde .Head of the Computer Department, and all other faculty members who provided us with valuable insights and feedback. Finally, we extend our thanks to all the participants who willingly contributed their time and data to this study.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

REFERENCES

[1]. S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, ``E-voting system using blockchain technology," in Proc.2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 113_117, doi: 10.1145/3376044.3376062.

[2]. B. Shahzad and J. Crowcroft, ``Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477_24488, 2019, doi: 10.1109/ACCESS.2019.2895670. [3] F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson, ``Blockchain-based E-Voting system," in Proc. IEEE 11th Int. Conf. CloudComput. (CLOUD), Jul. 2018, pp. 983_986.

[3]. M. S. Farooq, M. Khan, and A. Abid, ``A framework to make charity collection transparent and auditable using blockchain technology," Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106588, doi: 10.1016/j.compeleceng.2020.106588.

[4]. N. M. Crosby, P. Pattanayak, S. Verma, andV. Kalyanaraman, ``Blockchain technology Beyond bitcoin," Sutardja Center Entrepreneurship Technol., Univ. California, Berkeley, CA, USA, Tech. Rep., Oct. 2015. Accessed: Jan. 24, 2018. [Online]. Available: http://scet.berkeley.edu/wpcontent/ uploads/BlockchainPaper.pdf

[5]. T. Dimitriou, ``Ef_cient, coercion-free and universally verifiable blockchain-based voting," Comput. Netw., vol. 174, Jun. 2020, Art. no. 107234, doi: 10.1016/j.comnet.2020.107234.

[6]. S. Shah, Q. Kanchwala, and H. Mi. (2016). Block Chain Voting System. Economist. [Online]. Available: https://www.economist.com/sites/default/_les/northeastern.pdf