Grenze International Journal of Engineering and Technology, Jan Issue

Secured and Transparent Voting System using Blockchain Technology

Sujata Khairkar[1], Atharv Yeole[2], Asmita Pawar[3], Sakshi Londhe[4] and Santosh Warpe[5]
[1-5]MIT Academy of Engineering, School of Computer Engineering & Technology, Pune, India
Email: {smkhairkar, ayyeole, aapawar, salondhe, stwarpe }@mitaoe.ac.in

***Abstract*—This paper presents the Voting System using Blockchain Technology. It mainly focuses on the decentralized way of voting system for the corporate elections and can be expanded further for the democratic countries like India for a trustworthy election process. In this paper, Ethereum Blockchain along with other technology stack namely Truffle, Ganache, Metamask and React is used for the development of the portal. The admin will add the candidates and their details who are willing to compete in the election. The voters need to register themselves on the portal and the admin will validate their identity. Ahead of starting the elections by the admin, the voters can cast their votes through the comfort of their place without any need to travel to the election booths. After the casting of the votes by every participant voter, the admin will stop the elections and the winner will be displayed.**

***Index Terms*— Ethereum Blockchain, Voting System, Corporate Elections, Ganache and Truffle.**

I. INTRODUCTION

Election is a known and accepted practice for deciding on a leader [3]. A secure and transparent process is essential for elections. There is also the intervention of a 3rd party or a group of people from the system to check and monitor the validity of the election. This document shows the way to eliminate this interference of third parties and introduces a decentralized way of voting, where a group of people will not monitor the progress of the election; but the public. This can be achieved using Blockchain technology. Blockchain is a decentralized peer-to-peer (P2P) network of nodes. The main purpose of using blockchain is to remove centralized control and intermediaries from the system [4]. And create a decentralized open ledger system. All votes cast by candidates are recorded in the public book. And, this record is permanent and cannot be changed i.e. immutable. It ensures that the casted votes cannot be changed at any condition. They are permanent records. Still, if someone wishes to manipulate the ledger, first they need to hack all the previous blocks before adding a new block, which is almost impossible because of the consensus mechanism of the blockchain [6].

II. LITERATURE SURVEY

According to S. Agbesi [1], the proposed system uses the Ethereum blockchain framework and is based on a permissionless blockchain architecture. To perform specific tasks, Ethereum smart contracts are also written and deployed on the blockchain. As blockchain is based on a decentralized P2P network, the blockchain database will be always distributed across multiple nodes, and each participant in the blockchain network (i.e. connected

Grenze ID: 01.GIJET.9.1.503

nodes) will share a same copy of the database thereby, providing the needed immutability required, because once the results are committed no one can change them without a new transaction.
The method provided by K. Patidar and S. Jain [2] is suitable for small-scale elections such as inside corporate houses, boardrooms, etc. The implementation uses smart contracts from Ethereum. The Truffle framework is used in this document to develop, test, and deploy smart contracts. Ganache is used as an Ethereum client for testing. Here, Meta-mask is used as a browser wallet.
In the words of I. A. Srivastava et al. [3], no exchange of currency or cryptocurrency is used which may create possibility of vote duplicacy which will result in erroneous results. High level security is not used for authentication in the project.
Concept of election is explained as the simple wallet transfer of a coin by S. Jain [2]. The blockchain types: permissioned and permission-less are explained, which helped us to make the right choice for selecting one for our project i.e the permissioned blockchain, which can be accessed only by users with permissions. In our case it is the admin. Also, ethereum account types: external and contract accounts are explained.
A. K. Tyagi et al. [5] suggests Aadhar Card to be used as an excellent way of user authorization. As Aadhar is Unique for each and every person, it will help to uniquely identify a person be it for corporate or general elections. With the use of Aadhaar Card for authentication can provide effortless participation of large people in India. System is presented as the Blockchain as a service (BaaS) based on Service as a Service (SaaS). But the drawback of this system would be that it would be effective only in India as Aadhar is provided only for the citizens of India.
R. Cooley et al. [6] proposes two blockchain-based voting systems: reuse and reinvention. The reuse system forked Ethereum to take advantage of its security and privacy benefits. The upgraded system created a new blockchain voting system that uses two separate chains. One is to check the voters and the other is to secure the votes. This study also demonstrates a proof of concept.
Prof. Sandeep Shiravale [10] suggests the use of blockchain for storing the private documents of individuals. It will aid in making the data more secure and reliable, minimizing the data loss and unauthorized access. The hash algorithms and the consensus algorithm collectively maintain the data integrity while providing authorization and authentication. The main focus of the paper is blockchain and the Identity Based Encryption management concept. This system allows the encryption of the user data along with their identity thereby preventing them from Identity theft and fraud. These two technologies combined together will result in a much more secure way of data storage and privacy protection of the user.
According to Prof. Shitalkumar Jain and Nehe M [11], the transactions made using nodes in the blockchain are digitally signed with the hash of the previous transaction and the public key of the destination node; this method ensures that transactions are tamper-proof. A block containing transactions will be authenticated by certain nodes. In blockchain, each page in a ledger of transactions forms a block. This block affects the next block or page through cryptographic hashing. In simpler words, when a block is finally completed, a special secure code is created which links to the next page or block, forming a chain of blocks, or block-chain.

III. METHODOLOGY

This system consists of voters, candidates and admin. Initially, the Admin of the project will have to enter his/her details in the system with the unique Metamask Account ID. Admin details include First Name, Last Name, Email, and Job Title or Position. Candidates can be added by the Admin with their Name and Campaign Slogan. Then Admin can start the election. After the start of an election, Admin will be able to register voters on the system. Until then, Admin will not be able to add voters to the system. Voters can be added to the system with their Name, unique Metamask Account ID and Mobile No. A list of voters and their total count will be visible in the application. After successful voter registration, admin can verify them by verifying their account details and information. Then, verified voters can vote for a registered candidate by logging in with their unique Metamask account ID. Only verified voters will be eligible to cast a vote. If voters vote for a candidate, a small fixed no of ethereum will be charged through their Metamask Wallet. Also, after the completion of the work, votes added to the candidate will be reflected in the final voting results.
Next, when a voter votes for a candidate, block information is sent to all nodes in the network, the nodes verify the block with an algorithm, and when the majority of nodes say so, a transaction is activated, and blocks are added with the blockchain. This will happen on the Ethereum main net. And in the case of a local blockchain, this transaction block is formed in Ganache, a local blockchain created for testing decentralized applications (dApps). A block contains the block number, production date and time, amount of gas used, transaction hash, sender account address, and recipient account ID.

where,
Block No - Sequential Block creation serial no in the blockchain,
Mining No - Unique no generated when a block is formed,
Amount of Gas - if refers to the cost necessary to perform a transaction on the blockchain network,
Transaction Hash - Hash created while verifying the transaction,
Sender Account ID - Unique Metamask ID for transaction in the network,
Receiver Account ID - Unique Metamask ID for transaction in the network.
Each next block of transaction will be linked to the previous block with its unique hash and the chain of blocks will be formed, which is known as Block-chain. This chain of blocks will form a decentralized network which cannot be tempered or altered at any cost. Any tempering and altering of values will change the hash and system will inform the other nodes in the network. And, hence the previous version of the chain of block will be continued by the network of nodes.

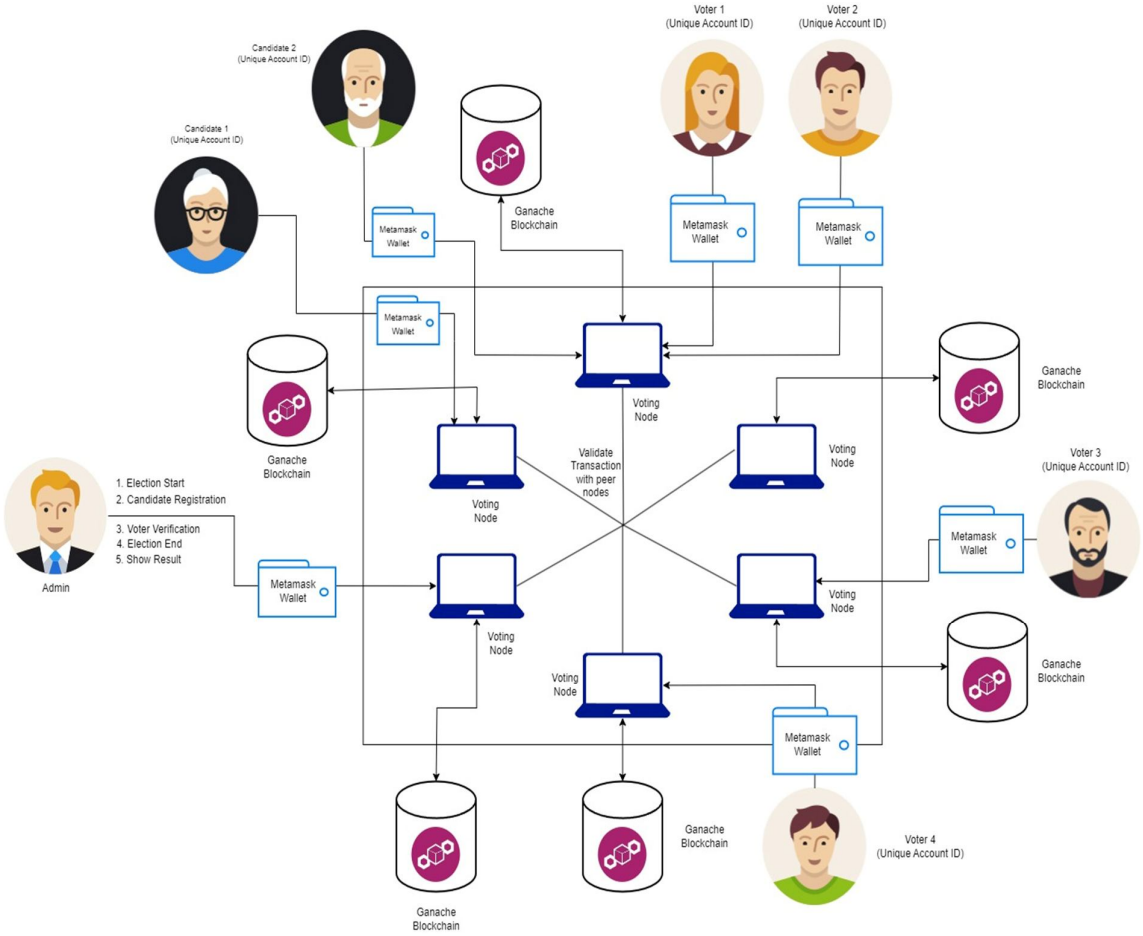

Figure 1. Architecture Diagram of a System

IV. Result & Discussion

This decentralized application (dApps) is built with the Ethereum Blockchain. Truffle suite is used in the implementation to test and deploy smart contracts to the blockchain. The truffle framework provides the environment for blockchain network and helps to develop, test and deploy the application. Metamask is a ethereum wallet which is used to make a ethereum transactions. The interface is built to use the Ethereum accounts to make the transactions. The ethereum smart contracts are written in Solidity for Elections. Ganache which is a part of Truffle suite, provides the local blockchain for development. It mainly used to test the decentralized application built on truffle.

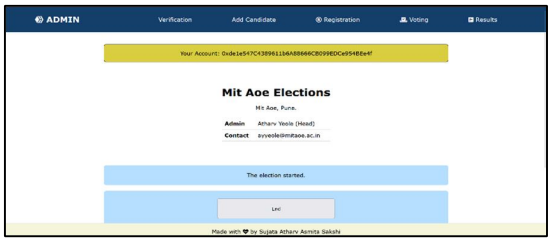

Figure 2. Admin Screen

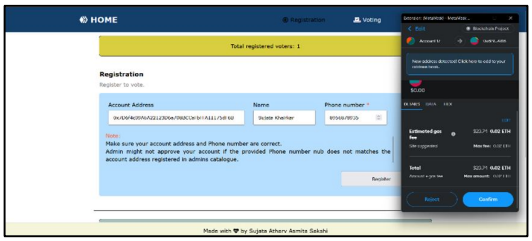

Figure 3. Voter Registration

Figure 4. Voting Screen

Figure 5. Election Result

V. Conclusion

The architecture of the solution we developed will eventually remember all the obstacles and limitations of the existing system and deliver the expected result. Voting is completely safe and transparent and visible to the voters. Blockchain voting is encrypted data that is completely open and stored on a blockchain network rather than on a single server. Although our system is diverse and fully open, we ensure the safety and protection of our voters. This means that anyone can count their votes by voting via the electronic blockchain, but no one knows who voted for whom.

Acknowledgment

The authors would like to thank Prof. Santosh Warpe, MIT AOE, Pune. for providing his valuable guidance throughout the process. Also we express our gratitude towards Prof. Ranjana Badre, dean SCET MIT AOE, Pune for all the timely academic support.

References

[1] S. Agbesi and G. Asante, "Electronic Voting Recording System Based on Blockchain Technology," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 2019, pp. 1-8, doi: 10.1109/CMI48017.2019.8962142.

[2] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[3] I. A. Srivastava, B. Saini, S. Phansalkar and S. Patwe, "Secure and Transparent Election System for India using Block chain Technology," 2018 IEEE Punecon, 2018, pp. 1-6, doi: 10.1109/PUNECON.2018.8745404.

[4] E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan and P. A. Sunarya, "Using Blockchain Data Security Management for E-Voting Systems," 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, pp. 1-4, doi: 10.1109/CITSM50537.2020.9268847.

[5] A. K. Tyagi, T. F. Fernandez and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 498-504, doi: 10.1109/ICECA49313.2020.9297655.

[6] R. Cooley, S. Wolf and M. Borowczak, "Blockchain-Based Election Infrastructures," 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1-4, doi: 10.1109/ISC2.2018.8656988.

[7] T. Vairam, S. Sarathambekai and R. Balaji, "Blockchain based Voting system in Local Network," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 363-366, doi: 10.1109/ICACCS51430.2021.9441912.

[8] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam and A. Islam, "Towards Blockchain-Based E-voting System," 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), 2018, pp. 351-354, doi: 10.1109/ICISET.2018.8745613.

[9] S. V., A. Sarkar, A. Paul and S. Mishra, "Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019, pp. 1075-1079, doi: 10.1109/ICCMC.2019.8819649.
[10] S. Khan, A. Jadhav, I. Bharadwaj, M. Rooj and S. Shiravale, "Blockchain and the Identity based Encryption Scheme for High Data Security," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1005-1008, doi: 10.1109/ICCMC48092.2020.ICCMC-000187.
[11] Nehe, M., & Jain, S. A. (2019). A Survey on Data Security using Blockchain: Merits, Demerits and Applications. 2019 International Conference on Recent Advances in Energy-Efficient Computing and Communication (ICRAECC). doi:10.1109/icraecc43874.2019.8995064.