Blockchain Based E-Voting System

Sakshi Vajre, Ashlesha Gomase, Megha Puram, Sakshi Vinchurkar
Department of Information Technology,
RTMNU, Nagpur,MH,India

Abstract- **Voting is the fundamental right for every nation. An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally, which makes the voting management task better than the traditional paper based method. Blockchain is a decentralized, distributed, public ledger that exists across the network. Blockchain-enabled E-voting (BEV) could reduce voter fraud and increase voter access. In this paper, the concept of developing an electronic voting system using blockchain technology is implemented. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The blockchain-based voting project has two modules to make the whole project integrated and work along. One will be the Election Commission who will be responsible for creating elections, adding registered parties and candidates contesting for the election added under the smart contracts. The other end will be the voter's module where each individual can cast a vote for their respective Assembly Constituency and the vote will be registered on the blockchain to make it tamper proof.**

Keywords - Blockchain, Ethereum, Decentralized, Distributed, Smart Contract.

I. INTRODUCTION

Elections are very important part of a democratic system enabling the citizens to express their views by voting and electing the best candidate for their Country. So the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain.

This paper provides a conceptual description of the intended blockchain-based electronic voting application and an introduction to the fundamental structure and characteristics of the blockchain in connection to electronic voting, here we discuss the electronic voting system using blockchain, a secure and robust system that ensures anonymity of the voter, transparency, and robust functioning. Blockchain- 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 Any proposed —new block‖ to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

II. LITERATURE SURVEY

1. Votereum:
An Ethereum-based E-voting system Khoi Cao-Minh, Chuong Dang-Le- Bao System empowered by Ethereum platform, including one server manages the entire system and the other handles all blockchain-related requests.[1]

2. Blockchain Based E-Voting Recording System Design:
G Bhavan, i —Survey on Blockchain Based E-Voting Recording System Design‖,2018, By adopting blockchain in the distribution of databases on e-

voting systems can reduce one of the cheating sources of database manipulation.[2]

3. Blockchain-Based E-Voting System:

Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, —Blockchain Based E-Voting System. 2018, School of Computer Science Reykjavik University, Iceland, this paper evaluates the potential of distributed ledger technologies.[6]

4. Blockchain and Its Applications:

A Detailed Survey: Supriya Thakur Aras, Vrushali Kulkarni, (2017). It explains how blockchain as a concept can be applied to a non-tokenized scheme. The paper also talks about blockchain taxonomy and how hybrid solutions become an obvious choice and moving from permission less to permission blockchain becomes imperative to solve certain kinds of problems where trust is paramount and a public permission less ledger seems both a risk and an overhead.[12]

5. Online Voting:

Voting System Using Blockchain: Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar,—Online Voting: Voting System Using B-chain ‖,2019, article gives a short review on various methodologies that are used in current voting.

The paper will help to build a system that will face the present and upcoming challenges and will remove drawbacks from these previous architectures.[7]

6. Decentralized Voting Platform Based on Ethereum Blockchain:

DavidKhoury, Elie F. Kfoury, Ali Kassem and Hamza Harb, 2018 —Decentralized Voting Platform Based on Ethereum Blockchain ,Department of Computer Science American University of Science and Technology, we propose a novel approach for a decentralized trustless voting platform that relies on Block-chain technology to solve the trust issues.

The main features of this system include ensuring data integrity and transparency, and enforcing one vote per mobile phone number for every poll with ensured privacy. To accomplish this, the Ethereum Virtual Machine (EVM) is used as the Blockchain runtime environment.[10]

7. Blockchain Based E-Voting Recording System Design:

Rifa Hanifatunnisa and Budi Rahardjo, 2017, —Blockchain Based E-Voting Recording System Designthis recording system occurs when the vote is over. Blockchain technology can be one solution to solve the problems that often occur in the electoral system. The use of hash values in recording the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable.[9]

8. Decentralized E-Voting System:

Venkata Naga Rani B, Akshay S, Arunkumar M. Ishwar Kumar M A , (2019)The main concept is to combine the technology of blockchain with Cryptographic Hash Function and Digital Signatures in order to realize the decentralized e-voting system with all the requirements of voting process without a trusted third party.[11]

III. EXISTING SYSTEM

In India, before 2004 there was a paper-based voting system. This is called as ballot Paper system. Voters had to go to polling booth and cast their vote by marking on seal in front of the symbol of a candidate for which they wanted to cast their votes on ballot paper. Results were announced by counting the votes.

The maximum vote gainer was declared as winner. India has population more than 120 crores. The ballot paper voting is not much reliable, time consuming and very difficult to count the vote and there are also problems like replacement of ballot paper boxes with duplicate, damage of ballot paper, marking stamp seal for more than one candidate hence there is a strong need to overcome these problems.

In order to overcome these problems Electronic Voting Machines Were introduced. By using EVM's, Votes are correctly recorded and there is no problem in counting, scalability, Accuracy, fast declaration of results and robustness of system. Main Problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing of booth by political parties, casting of votes by underage people and fraud voting may occur.

IV. PROPOSED WORK

There were a lot of studies carried to resolve the issues regarding the election process to improve it.

Here we have proposed existing online Electronic system integrated with the Blockchain Technology. Users' can vote from anywhere in the world until he possess a citizenship of the country. The voting is stored in the Blockchain which makes it tamper proof. As there's no standing in queue for casting vote it will save a lot of time and reduce the workload. For our architectural design we tried to create a system that doesn't entirely replace the current voting system but rather integrates itself within the current system which we are using today. We decided to do this because the majority of people are familiarized with the current system and the introduction of a new system can create confusion as well as disinterest.

As we are using Blockchain Technology, let's understand the important components of the architecture

- Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);
- Transaction: It is the blockchain system's smallest building block (records and details), which blockchain uses;
- Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
- Chain: A series of blocks in a particular order;
- Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;
- Consensus: A collection of commands and organizations to carry out blockchain processes. Characteristics of Blockchain Technology:
- Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved;
- Immutability: Any blockchain documents cannot be changed or deleted;
- Provenance: It refers to the fact that every transaction can be tracked in the blockchain ledger; • Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process;
- Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system;

- Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network. This proposed system uses some tools namely Ganache, Truffle Framework, Metamask, NPM. Truffle imports the smart contracts while Ganache uses internal Blockchain which can be accessed using Metamask with some Ether. For writing some contracts or transaction on blockchain user need to pay some amount which is in the form of Gas Fee. Once the vote is cast the mining process is completed by miners to create the block on the blockchain network, There are no of miners who compete with each other to complete the transaction. The miner who succeed in the transaction, awarded with the Ether paid by user to vote.

Dependencies used in this proposed system are as follows:
- Npm (Node Package Manager) Npm manages install, updates or uninstalls Node.js packages in an application. It is a command line based tool.
- Truffle Framework Truffle is a powerful tool to work with Ethereum smart contracts, provides testing platform for automated contracts, and manages networks and packages.
- GanacheIt is a virtual blockchain provide by Ethereum provides 10 standard accounts with their addresses and private keys along with 100 ethers in each account.
- Metamask It is a open source, user friendly tool having a graphical user interface doing transaction in Ethereum. Metamask is a bridge between Browser and Ethereum Blockchain.
- Solidity It is high-level language with JavaScript style syntax for contracts. It is a method for generating EVM machine level code and converts it into simple instructions.

V. PRODUCT FEATURES

- Eligibility: This property states that only eligible users can vote. Those who are provided with authentication the Election Commission.
- Privacy: Privacy is one of the most important aspects of democratic voting. Voters privacy should be maintained. No one should be able to know how a particular person voted or to whom the particular voter voted.

- Coercion resistance: No one should be able to force the voter and should not havethe ability to distinguish between whether the voter voted the same way he/shewas instructed to vote.
- Verifiability: This property states that everyone involved in the voting process should be able to verify the results. This brings transparency in the election. Also, an individual voter should be able to verify whether his/her vote is counted or not.
- Immutability: The voter's vote should be immutable. No one should be able to change the vote of any voter without proper concern of the voter. 5. Working of the System The voter will first visit the election Website. And make sure to log in into the chrome extension of Metamask to connect with the local Blockchain. Once connected the page is refreshed and the user will see the list of candidates and the current votes.

Voter just need to select the candidate name from the given list and click on the vote button provided at the bottom. The vote will be added to the selected candidate provided that the voter has not voted before. User can not cast their vote twice, it will show that you have already voted message. The local Blockchain is deployed using Ganache and Metamask is a set up to connect with it. Truffle framework allows to migrate smart contracts made on Solidity language to the local Blockchain.
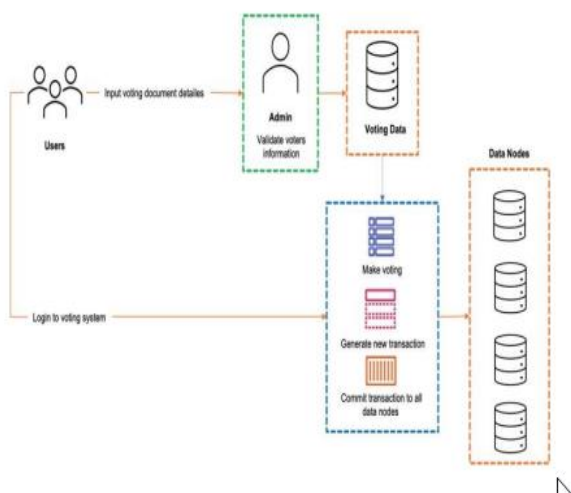

Fig 1. Voting Process Overview.

When user click to vote, Metamask allows to move Ether from one account to another, Every account in Ganache has an address and the private key using which user can log into the Metamask, each account has 100 ethers. As mentioned earlier voting needs some transaction fees which is gas fees, so from user's account some ether will be deducted as the gas fees and user will notified with transaction and the vote will be casted. This all transaction is visible to all severs of Blockchain. Voters can cross check their vote. Here Ganache is auto mining blocks.

Data Security Security is about risk management, so it is important to start with an understanding of the risk associated with the blockchain solutions. The specific risks of a blockchain solution depend on the type of blockchain being used. Let's take a look at the various types of blockchains with decreasing level of risks and increasing levels of security:

- Public Blockchains are public and anyone can join them and validate transactions. They are generally riskier. This includes risks where anyone can be part of the blockchain without any level of control or restrictions.
- Private blockchains are restricted and usually limited to business networks; membership is controlled by a single entity (regulator) or consortium.
- Permissioned blockchains allow the ledger to be encrypted so that onlyrelevant participants can see it, and only those who meet a need-to-know criterion can decrypt it. Performance Requirements The system is expected to have a reasonable short time of response. The voter should be able to import his/her wallet provided by the Election Commission within few seconds keeping in the mind the condition of network stability. The system's performance is different according to its modes:
- Election Mode: In this phase, the expected time to deploy the smart contracts totally depends upon the miners connected to the blockchain and the amount of GAS we decide to sign off the transaction to marked as validated one but as we are working locally, it is just a matter of half aminute or so.
- Voting Mode: In this phase, the system will be responding within seconds as we don't have to sign off transaction just to fetch the list of candidates for the elections but depending on the network stability andweb3 connection the above performance might be delayed. Next, after casting the vote it might take a minute or two to sign off the transaction depending upon the miners and GAS limit. Security Requirements:
- The data transaction between client and the blockchain server must be done over https to avoid mixed content attack.

- The reentrancy on a single function has to be minimized while deploying thesmart contract.
- To address the integer overflow error, the idea of counting the votes has been done within a specific event responsible for it.

Table 1. Software Requirement.

Software	Type	Version
Ganache	Ethereum Blockchain Server	2.4.0
Metamask	Ethereum Wallet	7.7.9
Truffle	Development framework for ETH	5.1.31
Node	JavaScript Runtime	12.17.0
Visual Studio Code	Integrated development environment	1.46

VI. CONCLUSION

As discussed Previously Current Election process has a lot of Malfunctions as well as the existing E-voting machines also have some issues like technical problems, not working properly, not secure, etc. But now the Blockchain Technology is extremely helpful for current scenario. Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness.

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this paper we have discussed the development of the Blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. It outlines the systems architecture, the design, and a security analysis of the system.

REFERENCES

[1] L. V. -C. -. Thuy, K. Cao-Minh, C. Dang-Le-Bao and T. A. Nguyen, "Votereum: An Ethereum Based E-Voting System," 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), 2019.

[2] Bhavani, G. (2018). Survey on Blockchain Based E-Voting Recording System Design. International Journal of Innovative Research in Science, Engineering and Technology, 4(11 November).

[3] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[4] Wikimedia Foundation. (2022, May 9). Electronic voting. Wikipedia. Retrieved May 10, 2022, from https://en.wikipedia.org/wiki/Electronic_voting.

[5] Tambare, R., Dixit, P., &Gehlot, R. S. (2021). Electoblock: A Secure Digital Voting System Based on Blockchain Technology. International Journal of Science, Engineering and Technology, 5. https:// www.ijset.in/wpcontent/uploads/IJSET_ V9_issue3_307.pdf

[6] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/ CLOUD.2018.00151

[7] Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and PranaliShirke Prasad Halgaonkar, ―Online Voting: Voting System Using B-chain‖,(2019), Online Voting: Voting System Using Blockchain

[8] Jafar, Uzma& Aziz, Mohd&Shukur, Zarina. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors. 21. 5874. 10.3390/ s21175874.

[9] Design: RifaHanifatunnisa and Budi Rahardjo, (2017), Blockchain Based E-voting Recording System.

[10] David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb, (2018), Decentralized Voting Platform Based on Ethereum Blockchain McCorry, P., Shahandashti, S. F. and Hao. F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[11] Venkata Naga Rani B, Akshay S, Arunkumar M, Ishwar Kumar M A, (2019), Decentralized

EVoting. System, International Research Journal of Engineering and Technology.

[12] Supriya Thakur Aras, Vrushali Kulkarni, (2017) —Blockchain and Its Applications – A Detailed Survey, International Journal of Computer Applications, Pune, India.