Blockchain Based Electronic Voting System

Deeksha M[1], Keertana Ganesh Ganiga[2], Lavanya D M[3], Nivedita Magadum[4], Sinchana K N[5]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Alva's Institute of Engineering and Technology, Mangalore, India
deeksha_m@aiet.org.in[1], keertanaganiga@gmail.com[2],
lavanyamurthy12@gmail.com[3], nsmagadum1006@gmail.com[4], sinchanaknagaraj@gmail.com[5]

Abstract: *The use of technology has grown increasingly significant in meeting human needs. Due to the increased use of technology, new obstacles have arisen in the democratic process. The majority of people today do not trust their leaders, holding elections is criticalin modern democracy. The biggest difficulties in the existing voting system are vote rigging, EVM (Electronic voting machine) hacking, election manipulation, and polling booth capturing. Smart contracts are meaningful pieces of codes, to be integrated in the blockchain and executed as scheduled in every step of blockchain updates. E-voting, is another trending, yet critical, topic related to the online services. The blockchain, togetherwith smart contracts is a promising contender for developing safer, cheaper, more secure,transparent, and easier-to-use electronic voting systems. Ethereum and its network are oneof the most ideal because to its consistency, widespread use, and provision of smart contract logic. An e-voting system must be secure, as it should not allow duplicated votesand be fully transparent, while protecting the privacy of the attendees. In this project abstract we have addressed the application of an e-voting application as a smart contract for the Ethereum network using the Ethereum and the Solidity language along with JavaScript UI.*

Keywords: Blockchain, Cryptocurrency, Ethereum

I. INTRODUCTION

This Indian Election System for study and tries to propose a solution for the Indian ElectionSystem by limiting the scope. The most important principle that defines an election is that they must represent the free expression of the will of the people. This kind of expression is only possible if the elections are accountable, transparent and inclusive. These principles arepiled by several by various electoral process-related obligations and various key-rights and freedoms. Voting whether conducted through the traditional ballot or via electronic means forms the basis on which democracy depends. With the rise in technological impact on the youth of the country and the various anomalies faced by the current electoral process, using technology to modify the existing process is necessity of the hour, Electronic Voting has taken center place in research with the intention of minimizing the cost associated in settingup the voting process, while ensuring the electoral integrity is maintained by fulfilling privacy, security and compliance requirements. The current method, whether electronic or not has proved to be unsatisfactory with respect to transparency. It can be very difficult for the voters to be assured that the vote he/she has casted during the election reflects in the election result.

Electronic voting using Direct Recording Electronic do not generate receipt on successful casting of votes. No record of election except vote count is made public by thegovernment, which means that the voters are not assured of any external interference in caseof government conducting the process of vote recounting. Replacing the traditional method with electronic method using Blockchain technique has the ability to prevent potential fraudsthat may take place during election. Blockchain technology is a distributed network of interconnected nodes. A copy of distributed ledger is assigned to each node, each of which contains a complete history of all the transactions that have been processed by the network. Each transaction processedgenerated a hash. The hash created depends not only on the current transaction but also on the hash of the previous transaction. Thus, any small change on the data will impact the hashof the transaction. If a transaction is approved by a majority of nodes it is written to the block.This allows the users to remain autonomous while using the system. A basic analysis of Blockchain suggests that it provides the potential of making the voting process more secure and reliable.

1.1 Building Trust with Blockchain

- **Distributed**: The distributed ledger is shared and updated with each incoming group action among the nodes connected to the Blockchain. All this can be worn out real time as there's no central server dominant the information.
- **Secure**: There is no unauthorized access to Blockchain created attainable through Permissions and Cryptography.
- **Transparent**: As a result of each node or participant in Blockchain contains a copy of the Blockchain information, they needaccess to all or any group action information. They themselves will verify the identities while not the requirement for mediators.
- **Consensus-based**: All relevant network participants should agree that a group action is valid. this can be achieved throughthe utilization of agreement algorithms.
- **Flexible**: Good Contracts that are dead supported bound conditions may be written into the platform. Blockchain networks will evolve in pace with business processes.

1.2 Benefits of Blockchain Technology

- **Time-saving**: No central Authority verification is required for settlements creating the method quicker and cheaper.
- **Cost-saving**: A Blockchain network reduces expenses in many ways in which. No would like for third-party verification. Participants will share assets directly. Intermediaries are reduced. group action efforts are reduced as each participant containsa copy of the shared ledger.
- **Tighter security**: nobody will temper with Blockchain information because it is shared among a lot of Participants.

1.3 Problem Statement

Current voting systems like ballot voting or electronic voting suffer from various security threats such as DDoS attacks, polling booth capturing, vote alteration and manipulation, malware attacks, etc., and also require huge amounts of paperwork, human resources, and time. This creates a sense of distrust among existing systems. So, a decentralizedvoting system using blockchain which can vote anytime/anywhere (During Pandemics like COVID-19 where it's impossible to hold election physically), Secure, Immutable, Faster, Transparent.

1.4 Objective

The Blockchain is a powerful technology that can improve the efficiency of voting systems. Blockchain voting is similar to traditional voting methods. In both cases, the same concepts and processes apply. To vote digitally, citizens must register and prove their citizenship in a particular jurisdiction. Record your ID and citizenship on the blockchain associated with that user's key. If the blockchain succeeds in making votes transparent, it will track and count votes in real time and elections can take place in a much shorter time.

II. LITERATURE SURVEY

Paper titled "A Secure and Optimally efficient Multi Authority Election Scheme" proposeda multi-authority secret-ballot election scheme that would guarantee robustness, universal verifiable, and privacy. where voters will participate using a computer, and the main consideration is the voter's efforts. In this system voters cast their ballot on a bulletin board. The bulletin board works with extended memory such that any part can access its content but won't be able to modify the data. The ballot does not contain any information about the vote itself but it does have an acknowledgment that it is a valid vote. The final tally is done when the deadline is over can be verified by any individual against the product of all submitted votes.This ensures verifiable due to the encryption method used [1].

Paper titled "A Smart Contract f or Boardroom Voting with Maximum Voter Privacy" had proposed the internet voting protocol with decentralized features and maximum voter privacyusing Open Vote Network (OVN). The OVN is a smart contract for the Ethereum Blockchain. However, the researchers soon found out that OVN is susceptible to DOS attacks. It could alsosuffer through traffic jams during the transaction which could delay the voting process for a longer time.

Hence this implementation is successful for boardroom meetings with a major drawback that each individual who wishes to vote needs to download the entire copy of the network [2].

Paper titled "Blockchain Based Voting System Can Better the Way of Elections in India" proposed a system for the Indian Election System based on the Hyperledger Network. The booth agents at different polling booths act as different nodes. These agents are selected by theElection Commission of India. For each phase, the consent of 5 nodes is to be considered. Membership Service Provider is also present on polling booths which helps to authenticate thevoters and generate public and private keys. Here they have suggested having three phases. During the preparation phase, a voter has to go to the nearest authorized voting center and register with his credentials so that his name is included in the Hyperledger network [3].

Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong in theirpaper "Performance Analysis of Private Blockchain Platforms in Varying Workloads" compared the two most popular Blockchain technology platforms viz Ethereum and Hyperledger. They developed an application that can transfer money from account A to account B. On comparing execution time, they found that as the no of transactions increases, the execution time increases. However, Hyperledger's execution time is always less than that of Ethereum.On comparing latency it was found that on less no of a transaction, Ethereum's latency is 2x times that of Hyperledger. Also, on varying no of transactions the change of average throughput of Hyperledger is relatively larger than that of Ethereum [4].

According to Denis Kirillov, Vladimir Korkho, Vadim Petrunin, Mikhail Makarov in their paper "Implementation of an E-Voting Scheme Using Hyperledger Fabric PermissionedBlockchain" proposed a system that can integrate traditional paper voting with blockchain technology which increases the trust among the participants. The systems that are developed to caste the vote by means of digital approach using online portals and electronic devices use various encryption and decryption techniques to guarantee the secure data transaction Due to rapid development of ledger-based technology and their potential to solve existing problems a modified version of the earlier developed protocol is being cited in this paper [5].

2.1 Existing System

Vote casting device referred to as ballot paper device in India. Voters needed to visit pollingsales spaces and solidify their vote with the aid of using marking on seal in the front of the image of a candidate for which they desired to solidify their votes on ballot paper. Results havebeen introduced with the aid of counting the votes. The most voted winner was declared as the winner.

India has populace greater than one hundred twenty crores the ballot paper vote castingisn't a great deal reliable, time ingesting and really hard to be counted number the vote and there are additionally troubles like harm of ballot paper, alternative of ballot paper containers with reproduction marking stamp seal for multiple candidates consequently there may be a sturdy want to triumph over those troubles.

In order to conquer those troubles Electronic VotingMachines Were introduced. Both the devices are connected through a 5m cable and one stop of the cable is completely fixed to the ballot unit. The managed unit has a battery percentage inside, which motorizes the device. The ballot unit has sixteen candidate buttons and the unused buttons are protected witha plastic covering tab in the unit. An extra ballot unit may be used when there are greater thansixteen candidates. The extra ballot unit may be related to a port on the bottom of the primaryballot unit. EVM's across the world are called DREs (Direct recording Electronic). EVMs are universally utilized in India because of the widespread elections of 2004. They had been utilizedin all of the meeting polls and widespread elections of 2009. By the usage of EVMs, Votes are correctly recorded and there may be no hassle in counting, scalability, Accuracy, speedy assertionof effects and robustness of device.

Main Problem lies in authentication, the man or woman whois vote casting might not be the valid man or woman. Problems like sales space taking pictures with the aid of using political parties, casting of votes with the aid of using underage humans and fraud vote casting can also additionally occur. A man or woman is supplied with the voter identity identification card as evidence of identity, issued with the aid of the Indian government. Lot of troubles are visible in voter identity notification playing cards like misprinting of name, missing of name, no clean picture graph identity

identification card, etc.

2.2 Proposed System

It is a private blockchain for instant Ethereum and Corda allotted software development. Used toset up a personal Ethereum blockchain which mimics the real international blockchain and whichhelps you to execute commands. run tests, and test our united states of America on the identical time as controlling how the blockchain works. It comes with flavour's: technologies to improve elections. These studies talk about various risks involved in adopting e-voting systems such as software challenges, corrupt volunteers, network bandwidth, and the challenges of hackers. We'veproposed to design the existing e-voting system integrated with the Ethereum Blockchain technology. The proposed system has the following advantages as compared to the existing system:

- Users will have unique ids so double voting is not possible.
- The voting transactionsare stored on the Ethereum Blockchain which are unchangeable which makes it tamper proof. Inthe proposed system, a smart-contract which will be written in Solidity language which will contain the logic of the voting process.
- Smart-contracts once written will be compiled using truffle which will generate byte code. Once the contract is compiled and deployed on theblockchain, it is not possible to make changes in the contract.
- This compiled contract can be accessed using web3.js which allows access to the variables and methods in the contract and interacts with the smart-contract. Admin login will be used to add candidates which will be appearing in the election. Voters able to register themselves on the portal using the registration process. Admin will verify the details of registered users and only the users with valid credentials will be able to vote in theelection A Meta mask account will be used to perform the above transactions.
- Admin will have the authority to decide the duration of the election. While the election is live on a portal, a voter can vote for a candidate only once (this is ensured by the constraint in solidity code which is deployed on blockchain which is non-mutable).

III. TECHNOLOGIES USED

- **Ethereum:** Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you'll be able to write code thatcontrols digital price, runs precisely as programmed, and is accessible anyplace within the world.
- **Ropsten Ethereum test Network:** Ropsten is AN Ethereum testnet (or test network). Testnet are generally utilized by developers to run "tests" for his or herapplication or software system. Currency on testnet is worthless.
- **Truffle:** Built-in good contract compilation, linking, preparation, and binary management. Automated contract testing for speedy development. Network management for deploying to any variety of public & non-public networks. Truffle documentation: https://www.trufflesuite.com/docs/truffle/overview
- **Web3.js:** Web3.js could be an assortment of libraries that enable you to act with a neighborhood or remote Ethereum node,victimization, and protocol, or IPC association.
- **Ganche:** Infura provides the tools and infrastructure that enable developers to simply take their blockchain application from testingto scaled preparation - with easy, reliable access to Ethereum and IPFS.

3.1. Methodology

- Admin will add the voter.
- The voter has to verify himself by his Aadhar with registered number.
- After successful login the voter will be directed to the page where he can see the participator of election and vote to his favourite
- After each vote the block is created and added to the chain of blocks with time strap
- As this is Immutable the voter can't revote once it has done.
- Finally, the result will be displayed after completion of election
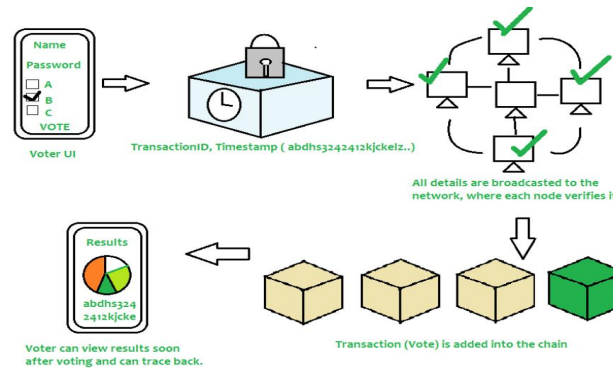
Figure 3.1 Methodology diagram

A model may be a complete, basic, and simplified description of software system design that consists of multiple views from a selected perspective or viewpoint as shown in Figure 3.1 A read maybe an illustration of a complete system from the attitude of a connected set of issues. it's accustomed to describe the system from the point of view of various stakeholders like end-users, developers, project managers, and testers.

3.2 Use Case Diagram

A use case diagram in the Unified Modelling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. A use case diagram is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. It can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. Use case diagrams are usually referred to as behavior diagrams used to describe a set of actions that some system or systems should or can perform in collaboration with one or more external users of the system (actors). Each use case should provide some observable and valuable results to the actors.
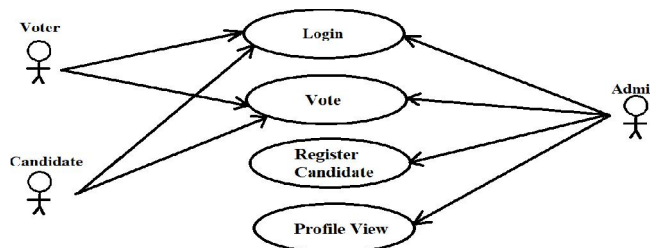
Figure 3.2 Use case diagram

Use Figure 3.2 displays the three individuals depicted in the use case diagram each have a distinct role to perform in the voting procedure. Candidates, administrators, and voters all play parts.

- Voters are able to log in and cast their votes.
- Internet voting is available for candidates.
- Administrators have the ability to add candidates, start the voting process, and log in to cast votes.

3.3 Work Flow

Figure 3.3 gives a clear picture of the workflow.

Step 1: Admin will add the voter

Step 2: The voter has to verify himself by his USN with registered number

Step 3: After successful login the voter will be directed to the page where he can see the participator of election and vote to his favorite

Step 4: After each vote the block is created and added to the chain of blocks with timestrap

Step 5: As this is Immutable the voter can't revote once it has done.

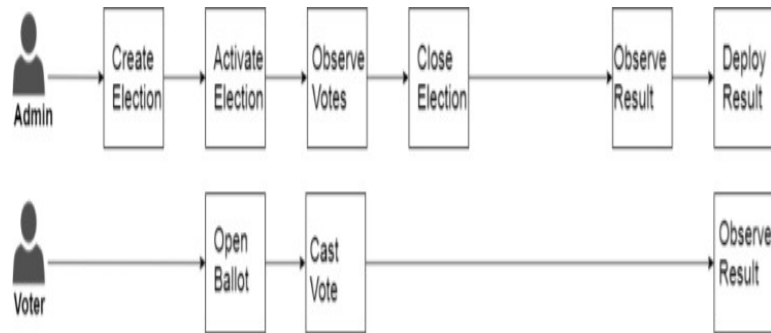Step 6: Finally, the result will be displayed after completion of election.

Figure 3.3 Work Flow

IV. CONCLUSION

Idea of harnessing the prowess of Blockchain to make E-Voting more secure and efficient has merit to it. Security and Convenience is the key that makes the user comfortable and also eliminates the barrier between the voter and voting system in any case where voting takes place. Blockchain as a technology makes it possible. Blockchain not only has the power to make the process more digitally transparent but also make it more secure by being immutable. In this paper, we have proposed and implemented a blockchain-based electronic voting system that utilizes hyper-ledger to conduct secure elections while guaranteeing users privacy. By comparison of Ethereum and Hyperledger, it has been observed that Hyperledger is more efficient than Ethereum in most of the performance metrics and also it being permissioned chain it allows to maintain privacy of the voter.

REFERENCES

[1]. "Supporting free and fair elections," https://www.usaid.gov/what-we-do/democracy- human-rights-and-governance/supporting-free-and-fair-

[2]. "Can blockchain change the election scenario in india?" Available at https://link.medium.com/kgJJ2No5F3, accessed: 2019-12-22.

[3]. S. Haber and W. S. Stornetta, "How to time stamp a digital document,"in Advances in Cryptology-CRYPTO' 90, A. J. Menezes and S. A.Vanstone, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991,

[4]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"Manubot, Tech. Rep., 2019.

[5]. G. Albeanu, "Blockchain technology and education," in The 12th Inter-national Conference on Virtual Learning ICVL, 2017, pp. 271–275.

[6]. S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Perfor-mance analysis of private blockchain platforms in varying workloads," in2017 26th International Conference on Computer Communication andNetworks (ICCCN). IEEE, 2017.