Implementation of E-Voting Using Ethereum Blockchain

Suraj Pawar, Roshani Pawar, Punam Dhomse

Students of B.E. in Information Technology
Department of Information Technology,
NDMVP'S KBTCOE Nashik, Pune University, Nashik, India

Abstract: The blockchain is the underlying technology behind the famous cryptocurrency Bitcoin and its successors and also triggering the start of a new era on the Internet and the online services. While many people focus only at crypto currencies. The blockchain is a very powerful tool for digitalizing everyday services, Due to the introduction of the smart contract, as in the Ethereum platform. Smart contracts are the meaningful pieces of the codes, which are integrated with the blockchain and which are executed as scheduled in every step of blockchain updates. Also, e-voting is another trending, yet critical topic which is related to the online of services. So the blockchain with the smart contracts is used to develop a safer, cheaper, more secure, more transparent, and easier-to-use evoting system. The main features of Ethereum and its network are the consistency, widespread use and provision of smart contracts logic. An e-voting system must be secure and it should not allow the duplication of the votes and also it should be fully transparent. In this work, we have implemented e-voting application as a smart contract using the ethereum wallets and solidity language. In case if people don't have ethereum wallets, they can use android wallets. After the election procedure, the records of ballots and votes will be held by Ethereum blockchain. The users can submit their votes using an Android device or from ethereum wallets. This creates a transparent environment, as well as reliability and efficiency of the voting system, is maintained.

Keywords: Blockchain; Ethereum; Smart-contracts; E-voting

I. INTRODUCTION

After widespread acceptance of Bitcoin, blockchain technology has emerged very rapidly and has become a trending topic in today's software world. Because of its high degree of transparency, blockchain technology can be used in many areas over time. For example, in the case of bitcoin there is no need for a central authority to approve or complete the operations on P2P based system. Hence the money transfer, as well as all structural information, can be kept in a distributed chain. The security is maintained using cryptological methods. Marriage certificates, medical information, banking information, etc., a lot of information can be recorded with this system. Ethereum coin which is emerged a few years after Bitcoin distinguishes the blockchain in the real sense. The software programs enforced by smart contracts can't be removed nor manipulated once written. So they can work properly and autonomously and transparently forever without any external stimuli. Hence blockchain technology is a very suitable solution for e-voting. E-voting system is being studied extensively, and many implementations are tested and used. But very few implementations are still in use and the reliable ones. As we all know democracy depends upon official elections. Hence a robust electoral process is most valued in democratic societies which provide transparency and privacy. Using sealed paper ballots, most government and many organizational elections are held, other questionnaires and poles are made on internet or SMS channels. The legacy paper-to-box voting creates some questions; how reliable are the notaries at hand? How can we verify the transparency? How can we be sure that the votes people gave are not changed before counting? How can we prevent the tricks that reduce people's trust in the poles? These and other similar problems have gradually entered a growth trend.

II. MOTIVATION AND RELATED WORK:

Motivation:

To provide a secure voting environment and to show that the reliable e-voting system is possible using blockchain is the main motivation of our in this project. The technology is very important in day to day life. As we all know that security is a big concern in today's technological world. So by using the technology we want to make our democracy secure. As our voting system is best but still there are many issues in our system. The latest example is the cryptocurrency that is Bitcoin.

As we know because of Bitcoin the transactions become very transparent. There is no need for the third party for any transaction of money. So the transaction has become more secure due to Bitcoin. The E-Voting system is recent technology in our India as it is developed already in other countries like Indonesia but it is still developing in India. So we thought to form such a transparent E-Voting system.

Related work:

Blockchain technology has been known as the underlying technology of cryptocurrencies, but nowadays it is further considered as a functional technology for improving existing technologies and creating new applications previously never practical. In this paper, we are focused on utilizing blockchain technology to introduce a new ID as a service (1IDaaS) for digital identity management. The proposed blockchain based ID as a service (IDaaS) is explained with one practical example that shows how the proposed BIDaaS works as an identity and authentication management infrastructure for mobile users of a mobile telecommunication company.

This paper explains the basic idea about the blockchain technology. The flow chart diagram is the basic information of how the blockchain works and also how this technology helps to overcome the different issues in the conventional voting system. It also

explains the experimental study of the e-voting system in Indonesia. Different blocks in the flow diagram tell how the verification is done and check whether the voter is valid or not.

 This paper shows an actual implementation of the E-voting system. For our design, we tried to create a system that doesn't entirely replace the current voting but rather integrates within a current system. We decided to do this to allow for as many different ways to vote as possible, this is so voting can be accessed by the majority of the population. .

III.METHODOLOGY AND DISCUSSION:

  In our system, The Ethereum platform is selected as the development platform for the voting blockchain application. In the blockchain development, Ethereum network provides a wide range of use cases, with the power of smart contracts. Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality. The ethereum comes with different functionality

•   **Open-source availability**: Ethereum is open-source. Every node in the blockchain stores the same data. Because anybody can build applications and products on top of the Ethereum blockchain. It's strongest value proposition their contracts can either utilize ether as a currency or they create and issue their own currency.

•   **Trusted**: With smart contract executions, every program executed on the blockchain is by a signed program, and no third party or middle-man is needed. Smart contract executions on the blockchain remove third-parties and middle-men. So that actually makes it trust less which makes it even more trusted. However, that contract data sits on-chain with Ethereum, meaning that the program is stored in the Ethereum blockchain itself, rather than just pointing to code that is sitting somewhere else.

To the development of an online voting system or elections, we need to solve many problems like transparency, authentication, and provability in a voting system. We need to assure people who attend the elections are real people and use correct credentials that we know in our system, and we should be able to prove that any time, also we need our elections are totally transparent. So, we need to gather and check signed and time-stamped data of the elections. Because nobody should be able to change the votes after they are cast. Also, we need individuality in elections, so that nobody can vote for someone else. These issues can be solved by using the blockchain peer-to-peer technology.

At any rate, use of the original Ethereum network for testing of experimental software related to the development of new smart contracts is costly but now a day these issue is solved by providing the remix editor for solidity. Remix, previously known as Browser Solidity, is a web browser based IDE that allows you to write Solidity smart contracts, then deploy and run the smart contract.

In our system, we defined the struct in solidity language like a voter, candidate, etc. The "Voter" is defined as a struct list of Voters and stores the data Voters in an array. Voters have some properties like isVoted, vote, and weight. The variable "isVoted" is a flag indicating that whether the voter has cast his vote already, or not yet "Vote" variable, likewise, stores the choice of the voter among all the candidates. In our system voter is mapped with the address so ID is an Ethereum wallet address associated with a voter account in the Ethereum network.

```
struct Voter {
        boolisVoted;
        boolhasRightToVote;
        uint8 vote;
        address ID;
}
```

In our system, we also defined the candidate as a struct which includes the properties like the name of the candidate and voteCount. The voteCount property stores the total number of vote gain of the particular candidate. This system also includes authorize () function which is used for authorizing the voter for voting without this the voter cannot put the vote. Our system includes the vote() function which used for a voter to put the vote into a system. This function checks whether the authorized voter will cast the vote or not. At the same time, we need to increase the vote count for the particular candidate. After all of this, the owner of the contract called the end() function then an election is over and counting of voting is done.

```
function authorize(address voter){
        require(msg.sender == owner);
        require(!voters[voter].voted);
        voters[voter].weight=1;
}


function vote(uintvoteIndex){
        require(now <auctionEnd);
        require(!voters[msg.sender].voted);
        voters[msg.sender].voted=true;
        voters[msg.sender].voteIndex=voteIndex;
        candidates[voteIndex].voteCount +=voters[msg.sender].weight;
}
```

Work Flow:
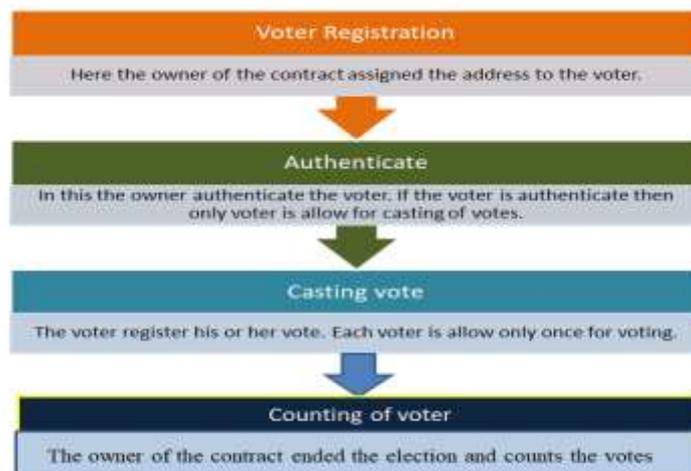
Following fig describes the workflow of the system.

Fig. Workflow of evoting system

System consists of different steps:

1)   Vote Registration:

This is process where the voter registers for voting. Voter must require the valid address to vote. Without address and address validation the voter is not able to vote. The voters select the candidate and vote accordingly.

```
function vote(uint voteIndex){
        require(now < auctionEnd);
        require(!voters[msg.sender].voted)
        voter[msg.sender].voted=true;
        voters[msg.sender].voteIndex=voteIndex;
        candidates[voteIndex].voteCount +=voters[msg.sender].weight;
                }
```

2)   Vote Authentication:

Authentication is require to maintain security issue. As the security is main concern which must be maintain. Authentication is done with the help of owner address. The owner validate the user according to address.

```
    function authorize(address voter)
                    {
                        require(msg.sender == owner);
                         require(!voter[voter].voted);
                         voters[voter].weight=1;
                    }
```

3)   Casting Vote:

The deciding vote cast by the presiding officer to resolve a tie. As the main motive behind this system is to protect our system form tampering the voting. After the voting, the same voter is not allowed to vote. In this, the owner plays an important role. If the Voter voted another time the vote is not considered again.

4)   Counting of vote:

To select the correct candidate form election vote counting process helps. Vote counting the main process for which the voting process takes place. In this system, voting is counted at the same time after the voting is completed.

IV. RESULTS AND DISCUSSION:

1.   Deploy the contract with the contract name and duration time.

Fig: Deploy contract.

2.   Add candidates with the help of Addcandidate function.

Fig: Candidate List

3.   After the successful addition of candidate authorized the voter with th

Fig: Authentication.

4.   After authorized, the voter gives the vote to the desired candidate with the string.

Fig: Vote.

5. After all, voting completed end the election.
6. Otherwise, election is ended according to the duration time we gave during the time of deploying the contract.
7. Now with the help of votecount function count the vote.

Fig: Vote Result.

V. CONCLUSION

This proposed smart contract of ours, we are going to move e-voting to the blockchain platform and also we have overcome some of the drawbacks or the fundamental issues of the legacy e-voting system, by using the benefits of the ethereum network and the blockchain structure. As a result of this work, the blockchain concept and the security methodology which it uses like immutable hash chains, has accepted to polls and elections. Blockchain applications are going to have an impact on every human aspect. At this point, Ethereum and the smart contract helped to replace the traditional voting system by the blockchain based voting system, which enables the global use of blockchain.

E-voting system is still a sensitive topic in the political and scientific area. Many technologies are invented to make the voting system secure, but many more failed to provide security and transparency to the voting. On the contrary, blockchain based voting system which uses the ethereum network and smart contracts provide the security like the privacy of voters, integrity, verification, validation, non-repudiation of the votes, and transparency of counting.

REFERENCES

[1] Rifa Hanifatunnisa , Budi Rahardjo, IEEE, 2017, Blockchain Based E-Voting Recording System Design, Bandung Institute of Technology.
[2] PavelTarasov and Hitesh Tewari, IEEE, 2018, The Future of E-Voting, University of Dublin .
[3] SafdarHussainShaheen, Muhammad Yousaf, MudassarJalil, IEEE,2018, Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain, Riphah International University.
[4] Ali KaanKoc , EmreYavuz, Umut Can abuk, GkhanDalkl, Towards Secure E-Voting Using EthereumBlockchain, DokuzEylul University , IEEE,2018.
[5] Baocheng Wang, JiaweiSuna,Yunhua He, Dandan Pang, Ningxiao Lu, IEEE, 2017, Large-scale Election Based On Blockchain.
[6] Jong-Hyouk Lee, IEEE, 2017, BIDaaS: Blockchain based ID as a Service, Senior Member.
[7] L. M. Bach, B. Mihaljevic, and M.Zagar, IEEE,2018, Comparative Analysis of Block chain Consensus Algorithm.