

Implementation of Voting System using Blockchain Technology

Mayur Shirsath, Mohit Zade,
Riteshkumar Talke, Praful Wake
Department of Information Technology
JSPM's Rajarshi Shahu College of
Engineering
Pune, India

Maya P. Shelke
Department of Information Technology
JSPM's Rajarshi Shahu College of Engineering
Pune, India

Abstract— Present voting system cannot be used and trusted for public elections as it creates a security problem, while offline elections require high cost. As a result, the old electronic voting could not be implemented on a large scale and hence the new system emerged, supported by blockchain technology. By using blockchain technology to vote online, the system can ensure privacy and transparency for each voter. And the voter's information and information compiled is stored in a distributed fashion. Because of its separation environment, blockchain-based legal systems are safer than a central server and internet-based voting system. During the research, an electronic voting system on ethereum was developed. With this system we can successfully solve the problem of fake voting by improving the reliability and safety of e-voting..

1. Introduction

Evolving Computer Science technologies have brought many changes in our day to day life, our democratic system needs to accept electronic voting in order to move forward. Central electronic voting systems emerged as another form of ballot paper, where voters can vote from any place hence increasing the voting percentage.

[1]. Because this system is prone to tampering and control of data, during the accounting process, the integrity of this e-voting cannot be

ensured due to the possibility of attack or fraud by third parties.

At the primary level, an electronic blockchain based voting system has been used. Each voting participant, being a member, keeps the integrity of voting results by having personal voting data and syncing it. In simple words, the data in the system is not centrally located. Making it difficult for anyone to deceive the information and block unauthenticated votes, ensuring voting honesty and credibility. All the processes involved in voting right from registration, voting and counting are regulated online [2]. Acquiring an electronic voting system is the highest priority of most countries and institutions [3]. In spite of having advantages of the current online voting system, in real life the offline voting system is still in use.

So, during the course of this study, an e-voting system based on blockchain technology was developed instead of a central server-based e-voting system with the help of distributed ledger technology. During this study, among the various available blockchain technologies, Ethereum was finalized and the e-voting system,

using smart contracts based on Solidity, the programming language of Ethereum, was developed.

2. Related Studies

2.1. Blockchain

All in all, a blockchain is a link to time-linked blocks that act as an immutable virtual type of storage. New innovations are added to mining but deleting or editing of currently existing operations is not possible. Each and every block consists of a hash value that is encrypted that is used to recognize the individual block[5]. Identity is decided by attracting the header of a block with the SHA-256 type of encryption algorithm. Blocks are made using the Merkle trees. Root of the Merkle tree can be called a hashtag to prevent the details of the process being distorted, which is done like a tree [6]. If we want to create a Merkle tree by doing A, B and C, after speeding up the data for each and every transaction, results are stored firstly in each location. For parent node creation, transactions named A and B i.e a 32-bit hash of child nodes, are joined together to produce a 64-byte unit of character, with a double hash that ultimately becomes a parent node hash. Likewise, until one of the nodes still remains at a high level, the statistics are continued. When all the actions are performed like a binary tree, the Merkle hash value is the last remaining hash value. Block hash value is used to verify the integrity of the title value and the Merkle hash value of the block is used to verify the integrity of the work. "Previous block" name is used to store the value of the pre-built block hash in the next item of the block[11]. As we know, blocks that contain the transactions are connected in sequential manner to a blockchain;a block hash value can be used as a blockchain link to create a new block[12].

2.2. Smart-Contract

Smart Contract is a piece of code that is stored on blockchain which gets executed when certain condition get's triggered.Intelligent contractors can "integrate user interaction and protocol" into a network in order to to automatically execute an agreement so that all participants can agree on certain outcome, without involvement of any middleman or time loss. Smart Contracts have many applications in financial purposes like trading , real estate trading, investing , lending , economic sharing and borrowing.Several research has been conducted in the field of system security using blockchain. Blockchain was evaluated as a viable technology in the real estate market and has impacted the real estate industry in a variety of ways, including offering a new means for buyers and sellers to connect with one another. Ethereum is an open platform that generates smart contracts in a blockchain network by transferring data to a code instead of money to generate code. Blockchain technology can be cost efficient as it will cut middlemans out of the transaction process. Ethereum is a decentralized, open-source blockchain(similar to bitcoin) with additional smart contract(written in solidity) functionality [13]. The smart contract is a code on the blockchain which can be seen using a unique address. Smart contracts is a kind of Ethereum account which means they have a balance and can perform transactions over the network.No one can control them as they function as they are programmed and deployed.User with accounts can interact with the functions defined in the smart contract by submitting transactions.With Smart Contract, we can define rules and automatically enforce them via code.Once created , it cannot be deleted by default and all interactions with them are irreversible. [15].

3. Implementation of the System

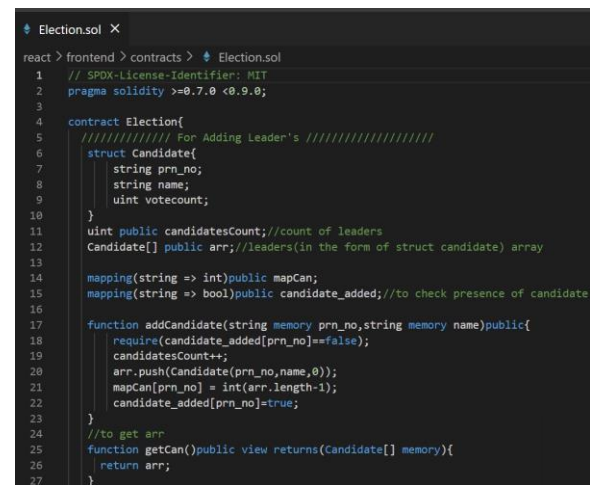
In this paper, we put forward the Ethereum based blockchain platform for the Electronic

Voting System. For testing the same study, we created a React.js web page. RPC-based test net environment was used to manage blockchain, on the other hand front-end and the Blockchain system integration was done with a Web3.js module. A smart contract was posted on the Ethereum blockchain network in order to make a vote. There is a separate contract holder in a distributed contract, which is a list of candidates, and votes received by each candidate. A candidate smart contract job is called when a particular voter votes for any particular candidate using a web browser. After the voting ends and the results need to be shown, a function used to calculate total votes is called. In this paper we are suggesting a new way to ensure site-based voting. This e-voting application creates a new voting account using a prn number and mobile number which the voter had at the beginning of the registration period. All voters are added into the Voters' contract at the time of registration. For encryption, the Advanced Encryption algorithm SHA256 is used. The SHA256 is widely used throughout the world because of its higher speed and security. Here, we use the SHA256 algorithm keeping in mind the security of the advanced nature of Blockchain-based processing of transactions and fraudulent transaction's prevention. Voters can first register on the portal using a unique prn number and mobile number and then login using the same credentials to access the system at the time of voting.

At the time of voting the voter first enters his/her prn and mobile number using which the voter registered during registration. An OTP is sent to the user for verification after which the voter is authenticated. After the authentication the voter is allowed to cast the vote only if the voter has not voted previously. The voters who are authenticated select a candidate from the given list of candidates for voting. The details of the candidate selected are then sent to the voting function in the smart contract. The function

performs a transaction and increments the vote count of the selected candidate. Every transaction being performed a new block is created, and a certain amount of gas must be paid. The blocks get added to the blockchain after the successful transaction. Post completion of the election, the results are declared on the result page. The result function in the contract returns the whole record of candidates along with the vote count.

In accordance with the principle of accuracy in an e-election, the voters have to participate in the voting process directly without involvement of any third party by providing a code which helps to ensure that it participates in election process using the personal information (phone number, etc.) of voter associated with the particular election.



```
1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.7.0 <0.9.0;
3
4 contract Election{
5     // For Adding Leader's
6     struct Candidate{
7         string prn_no;
8         string name;
9         uint voteCount;
10    }
11    uint public candidatesCount;//count of leaders
12    Candidate[] public arr;//leaders(in the form of struct candidate) array
13
14    mapping(string => int)public mapCan;
15    mapping(string => bool)public candidate_added;//to check presence of candidate
16
17    function addCandidate(string memory prn_no,string memory name)public{
18        require(candidate_added[prn_no]==false);
19        candidatesCount++;
20        arr.push(Candidate(prn_no,name,0));
21        mapCan[prn_no] = int(arr.length-1);
22        candidate_added[prn_no]=true;
23    }
24    //to get arr
25    function getCan()public view returns(Candidate[] memory){
26        return arr;
27    }
```

Fig. 1.1 : Smart Contract

```

28 /////////////////////////////////////////////////// For adding Voters ////////////////////////////////////////
29
30 struct Voter{
31     string prn_no;
32     string name;
33     bool voted;
34 }
35 mapping(string => bool) voter_presence;
36 uint public no_of_voters=0;
37 Voter[] private arr1;
38
39 function addVoter(string memory prn_no,string memory name)public{
40     require(voter_presence[prn_no]==false);
41     no_of_voters++;
42     arr1.push(Voter(prn_no,name,false));
43     voter_presence[prn_no] = true;
44 }
45 function getVoters()public view returns(Voter[] memory){
46     return arr1;
47 }
48 /////////////////////////////////////////////////// Voting ////////////////////////////////////////
49
50 mapping(string => bool)public votedornot;
51
52 function Vote(string memory leaders_prn,string memory voters_prn)public{

```

Fig. 1.2 : Smart Contract

```

48 /////////////// Voting //////////////////////////////////////////
49
50 mapping(string => bool) public votedornot;
51
52 function Vote(string memory leaders_prn, string memory voters_prn) public {
53     require(votedornot[voters_prn] == false);
54     require(voter_presence[voters_prn] == true);
55
56     arr[uint(mapCan[leaders_prn])] .votecount+=1;
57     votedornot[voters_prn] = true;
58 }
59 }

```

Fig. 1.3 : Smart Contract

[illegible]

Fig. 2 : Ganache GUI

Project Home Voter Registration Candidate Registration Voters Candidates Vote Result Capture

Voter Registration

First Name	<input type="text"/>	Last Name	<input type="text"/>
Videx		Kumar	
University PRN	<input type="text"/>	College Year	<input type="text"/>
8252889514		Final Year	<input type="text"/>
Mobile Number	<input type="text"/>	OTP	<input type="text"/>
+91		Send OTP	<input type="button" value="Send"/>
<input type="button" value="Submit"/>		Verify OTP	<input type="button" value="Verify"/>

Fig. 3 : Voter Registration

Project

Home

Vote Registration

Candidate Registration

Votes

Candidates

Vote

Result

Capture

Candidate Registration

First Name

Last Name

University PIN

College Year

First Year

Mobile Number

OTP

Send OTP

Send

Verify OTP

Verify

Submit

Fig. 4 : Candidate Registration

Project	Home	Voter Registration	Candidate Registration	Voters	Candidates	Vote	Result	Capture
---------	------	--------------------	------------------------	--------	------------	------	--------	---------

Candidates

University Pin	First Name	Last Name	Mobile Number	College Year
<input type="text"/>	Ritesh	Kumar	<input type="text"/>	Final Year
<input type="text"/>	Mayur	Shruthi	<input type="text"/>	Third Year

Fig. 5 : Candidates List

Project	Home	Voter Registration	Candidate Registration	Voters	Candidates	Vote	Result	Capture
---------	------	--------------------	------------------------	--------	------------	------	--------	---------

Voters

University Ptn	First Name	Last Name	Mobile Number	College Year
██████████	Pratik	Wade	██████████	Final Year
██████████	Mohit	Zack	██████████	Third Year

Fig. 6 : Voters List

[Project](#) [Home](#) [Vote Registration](#) [Candidate Registration](#) [Notes](#) [Candidates](#) [Vote](#) [Result](#) [Capture](#)

Vote here!

Pin Number

Mobile Number

OTP

Send OTP

Verify OTP

Send

Verify

Login

Fig. 7.1 : Voter Login Page

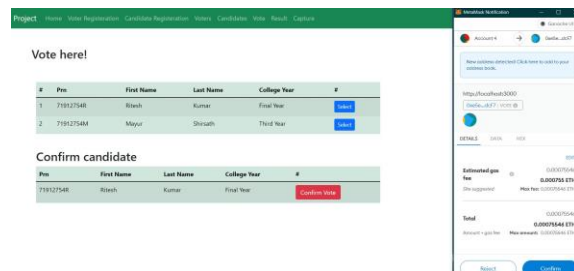


Fig. 7.2 : Vote confirmation Page



The screenshot shows the 'Result' page of the application. It features a table with columns for #, Pm, First Name, Last Name, College Year, and Vote Count. The table lists two candidates: Ritesh Kumar (First Year) with 0 votes and Mayur Shrivasth (Third Year) with 2 votes.

#	Pm	First Name	Last Name	College Year	Vote Count
1		Ritesh	Kumar	First Year	0
2		Mayur	Shrivasth	Third Year	2

Fig. 8 : Result Page

4. Conclusion

In this application, we have selected Ethereum blockchain technology to improve the e-voting system. The Solidity language based Smart Contract was developed and afterwards deployed on the ethereum blockchain to ensure the integrity of the counting of votes can be achieved in the e-voting system that we have developed. However, the system may have problems in future as contracts cannot be changed or updated once deployed. The contract is deployed on the blockchain through a metamask account and a specific gas is charged as a fee for deployment. Further, we suggest a plan to improve access and maintenance of smart contract development by analyzing the dissimilarity between the languages of Ethereum

i.e Solidity language of smart contract and the languages used for development of existing systems.

It is important that we ensure the confidentiality of each vote and also maintain transparency in the whole voting process. To provide such secrecy, honesty as well as transparency we must provide the voting system with a high level of security. The application used the most secure technology in blockchain to develop an e-voting system with limited local restrictions so that the

credibility in the whole process is ensured and the effects it has among voters. The research was done by studying the various approaches adopted in different sectors most notably in cryptocurrency. As the whole process can be monitored in real time by us, it provides a high level of reliability in an e-voting system and in consequent results. As a high level of security can be achieved in an e-voting system developed and also as a high level of loyalty can be promised to the electorate as well, it will result in the whole concept of online voting system being continued to be trusted by the voters.. Above application will promote participation in voting as well as facilitate online voting, thus achieving higher turnout of votes which in result will allow for making decisions for our modern society in a more democratic way.

5. References

- [1] Raghav Chhabra, Uday Vohra, Vishrant Khanna, Aditya Verman, Poonam Tanwar, Brijesh Kumar, “ The Next Gen Election: Design and Development of E-Voting Web Application”, Issue 10-12 June 2020, IEEE
- [2] Ramya Govindaraj, P Kumaresan, K. Sree harshitha, “ Online Voting System using Cloud”, Issue 24-25 Feb. 2020, IEEE
- [3] Bhushan M. Pawar, Sachin H. Patode, Yamini R. Potbhare, Nilesh A. Mohota, “ An Efficient and Secure Students Online Voting Application,” Issue 8-10 Jan. 2020, IEEE
- [4] Rajalakshmi Krishnamurthi , “A Brief Analysis of Blockchain Algorithms and Its Challenges”, Issue January 2021, ResearchGate.
- [5] Nizamuddin, N.; Salah, K.; Azad, M.A.; Arshad, J.; Rehman, M.H. Decentralized document version control using ethereum blockchain and IPFS. Comput. Electr. Eng. 2019, 76, 183–197.
- [6] Kim, C. An online voting system based on Ethereum block-chain for enhancing reliability.

J. Korea Acad.-Ind. Coop. Soc. 2018, 19, 563–570.

[7] Ko, Y.S.; Choi, H.S. Changing Business Paradigm and Its Application—Focused on the Block Chain Technology. Korea Sci. Art Forum 2017, 27, 27–28.

[8] Park, K.; Kim, C.; Youm, H.Y. Countermeasures against Security Threats to Online Voting Using Distributed Ledger Technology. J. Korea Inst. Inf. Secur. Cryptol. 2017, 27, 1201–1216.

[9] Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, “ Multi-purpose platform independent online voting system,” Issue 17-18 March 2017, IEEE

[10] Mrunal Annadate, “Online Voting System Using Biometric Verification”, Issue April 2017, ResearchGate

[11] Dukka Bindu Venkata Raghav, Sunith Kumar Bandi, “Digitized Electronic Voting System”, International Journal of Reconfigurable and Embedded Systems, November 3, 2016

[12] Jayesh Solanki , Divykanth Meva, “Comparative Study Indian Electoral Reforms in Indian Context”, Issue 27-28 Sept. 2019, IEEE

[13] Henry Rossi Andrian, Novianto Budi Kurniawan, Suhardi, “Blockchain Technology and Implementation : A Systematic Literature Review”.2018 International Conference on Information Technology Systems and Innovation (ICITSI) October 22-25,2018.

[14] Ashish Singh,Kakali Chatterjee,” Secure Electronic Voting System Using Blockchain Technology”,2018 International Conference on Computing, Power and Communication Technologies (GUCON) Sep 28-29, 2018.

[15] Mayur Shirsath, Mohit Zade, Riteshkumar Talke, Praful Wake, Maya P. Shelke, “Survey on Voting System using Blockchain Technology” International Journal of Engineering Research & Technology (IJERT), Volume 11 , Issue 4 , April - 2022