E-Voting using Ethereum Blockchain

Shubham Pareek[1], Anuj Upadhyay[2], Satya Doulani[3], Siddarth Tyagi[4], Aditya Varma[5]

[1,2,3,4,5]Students,
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Chennai

***Abstract*: Blockchain is now one of the most trending topic in the IT industry, but it is mostly about cryptocurrency hype, which is the limited use of blockchain so to exploit the potential of the blockchain technology, Ethereum came up with the concept of decentralized application. Ethereum provides a platform for development of decentralized application using ethereum virtual machine and test it in the virtual environment. What makes it more powerful is the introduction of smart contracts, Smart contract is the integration of meaningful code in the blockchain. Smart contract creates a virtual contract between the owner and the user which is applied to the blockchain so all the users have to agree to the contract which preserves the integrity of the blockchain, Smart contracts validates the use of the blockchain transactions. E-voting is a trending yet critical topic related to providing a reliable and secure online platform to cast votes. In a democratic country there is a high demand of a decentralized and transparent platform of voting. An E-voting platform must be secure, it should provide one person one vote policy, it should be transparent, easier to use. Ethereum and its wide spread network is the most suitable platform for deploying such application. The application can tested and deployed on a test platform using ethereum virtual machine(EVM) which provides a test network to test the application before deploying to the main ethereum network, When E-voting is deployed in the main network all the users can vote for the candidates, It provides a secure way of hiding the voters identity yet keeping the record distributed such that there is not a single point failure, It provides a P2P-based system there is no need of a third party having control over the process. The blockchain technology ensures the consistency and security of the application. In decentralized applications instead of using a single database a distributed database is used, the data is not stored in a single place and the data is not governed by a single party which makes it decentralized and the data is validated is used using cryptography and algorithms. As everyone is getting concern regarding their role in the election and in the transparency in election. A blockchain enabled e-voting platform is the only reliable solution to this problem.**

***Keywords*: blockchain; ethereum; smart-contracts, e-voting.**

1. INTRODUCTION

Every six out of ten country is a democracy. Election plays an important role in democracy. It gives the rights to the citizen to elect the leader and the country's representative, But the process of voting is flawed as the voting infrastructure is not using a proper architecture. The voting machines that are used in almost all the democracies are centralized i.e, a particular person or community controls and analyses the collected data from the voting process. Which makes the process vulnerable to many flaws in the system and lack of transparency to the voters. To overcome this situation and to empower the democracy the Blockchain technology can be used. The blockchain technology provides a decentralized and distributed architecture for development of applications. The ethereum community introduced the concept of decentralized applications which uses the blockchain technology to create an app. The major difference between a centralized and a decentralized application is, In decentralized application instead of using the traditional database at its backend the blockchain is used. Blockchain serves as the decentralized and distributed database system which uses cryptography for the storage of information which helps in storage of immutable data. The Blockchain technology provides a peer to peer communication and eliminates the third party. Initially the blockchain technology was used in cryptocurrencies but the introduction of decentralized applications have opened a door of opportunities for the exploitation of the blockchain technology.
As already mentioned, with its unique distributed , decentralized and distributed architecture the blockchain technology may resolve many issues in the digital age and it may help in the implementation of an e-voting platform which is not mostly used do to the presence of many threats in the web like hackers and security issues so with the introduction of decentralized application a secure, safe, decentralized and distributed e-voting platform can be implemented which will be free from all vulnerabilities and threats and yet keep the voters vote and identity intact.

2. CONCEPT

Currently the main challenge in a democratic country is to attract more people to participate in election process and do a fair voting. As the voter turnout is decreasing every year and the democracy is becoming weak. As the citizens do not believe in the electoral process. As the process is not transparent and is time consuming. Our main concern in this project is to provide a safe, secure and easy to use voting environment and show that a better alternative to traditional voting is e-voting which is possible by using blockchain technology. Because, when e -voting will be available for the public every eligible individual with internet connection and a phone or pc will have the power to vote and the process will be very less time consuming and secure and it will attract more voting and will increase the rate of turnout as the process will be simple and the identity of the voter is preserved. No matter wherever the person is the location of the individual does not matter there will be no geographical barrier and voters all over the country can vote at the comfort of their homes by registering themselves and they don't have to voting polls and waste

their time by standing in queue. Also the cases of corruption are more prevalent in during elections huge amount of money is wasted in this process. By using the blockchain technology this can be stopped because there won't be a single authority having total control over the process. This will fulfil the actual meaning of democracy.

The concept of e-voting is not new it is much older than blockchain. So that, all known e-voting processes have been done using a centralized authority having total control over the process. Estonia is an example, since the government of Estonia first implemented the process of online evoting. Which lead to increase in the number of voters voting. It was able to maintain the principle of one person one vote using id card authentication process but the process is not completely secure as many cybersecurity experts found loop hole in the process as the data is stored in a single database and the data can be tempered and changed. To overcome this challenge the blockchain proves to be very effective as the data are not stored in a particular database but spread across the network and stored using cryptography so it will provide a better alternative to a simple online evoting process.

3. COMPONENT

The prototype application was build and tested on test network it has the following component:

Back-end: The backend of the system is the blockchain architecture which is build using the solidity language. The solidity language uses the smart contract which makes a virtual contract between the system and user. The smart consists of code written in solidity language which is kind of object oriented language like c++ and c#.

Front-end: The frontend is build using html,css,javascript and web3 js. The layout of the webpage is done using html and css is used for designing the website. Web3 js acts as a bridge which makes a communication bridge between the backend and the frontend. It takes the bytecode from the solidity code after compiling is received by web3js and transferred to the test network to establish the connection.

Test Network: The test network ganache-cli was used to deploy and test the smart contract. Ganache-cli comes with ten ethereum accounts which hold some ether. This ether can be used for making transaction in the application . For every action performed in the blockchain application there is some amount of ether involved.

Metamask: Metamask plays an important role in transaction. Ether can be transferred from one account to another. It helps to handle the transactions.

Truffle compiler: Truffle provides a premium development environment, testing framework and asset pipeline for assets using the ethereum virtual machine, aiming to make the development of decentralized apps easier. It has built in smart contract compilation, linking development and binary management. Provides rapid application development. It provides console for communication with smart contract. It has external script runner that executes script within Truffle environment.

Linux terminal: The various commands and testing is done using the linux terminal. The terminal provides a very flexible platform for deploying the test commands and running various applications like the ganache-cli and the truffle compiler.

4. IMPLEMENTATION AND DISCUSSION

The Project is implemented on ethereum as the development platform and also the blockchain network. As ethereum provides a vast variety of tools which can be used in the development of decentralized apps. The ethereum community is a vast community of developers and they develop the platform of ethereum which provides the platform for development of applications. Ethereum provides ethereum virtual machine which provides a software development environment for decentralized apps.In Ethereum the blocks are made in real time and the blocks are validated by the miners. The miners solve a complex algorithmic problem which generates a nonce value which makes a link with previous block and by this process all the blocks are connected to form a blockchain. The data is stored in blockchain using cryptography. This provides the ideal platform for the purpose of our project.

The main concern in E-Voting is how to protect the users identity yet preserve transparency and integrity of data. To solve this problem ethereum provides the different hash values to users in the network through which it is almost impossible to identify the individual and the transactions done in the ethereum network is visible to everyone in the network and can be validated it makes it transparent to all the nodes in the network and to maintain the integrity of the data the data is not stored in a particular location but it is spread across the network which acts as a distributed database which makes the data immutable and very difficult to manipulate, By this process the integrity of the data is maintained. It provides a peer to peer communication where all the applications run on ethereum network. For the process of voting each voter must be provided a ethereum wallet which will consist of limited amount of ether which will be used to vote for the candidate and the votes will be recorded in the blockchain using the smartcontract which will validate and verify the voters and vote. The application is tested on the test network the metamask. Metamask provides number of network the one used in the project is custom rpc but for final deployement it should be deployed in the main network. The connection to the custom rpc is done by writing http://localhost:9545. As shown in figure2.

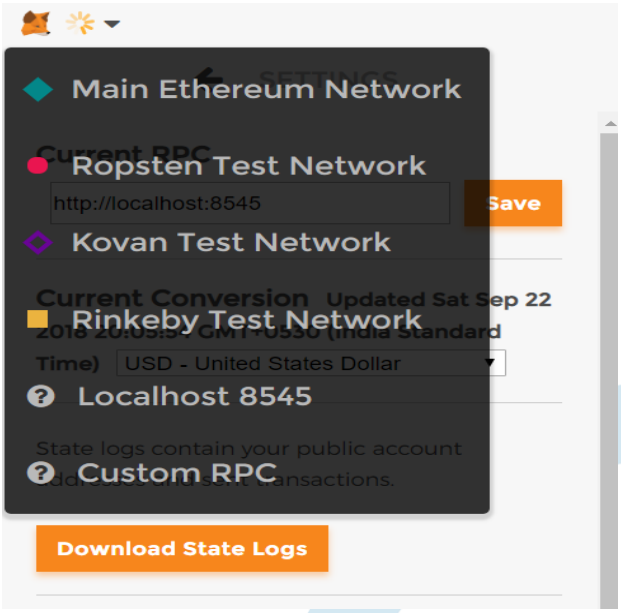

Figure1:

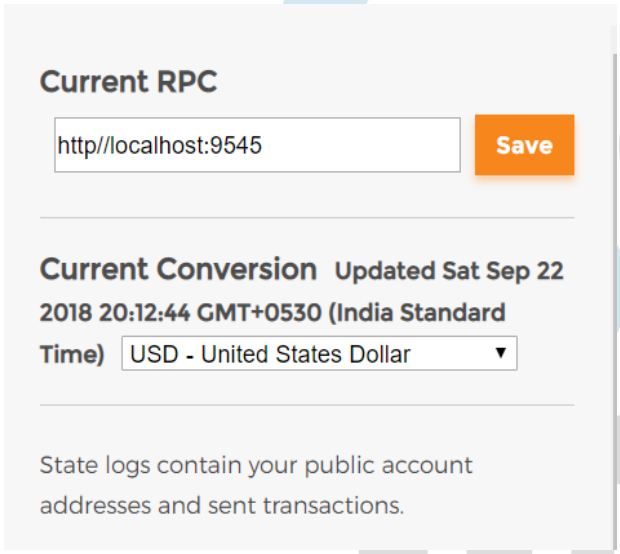

Figure2

In solidity programming in the first line of code we have to specify the version of solidity we are using there are many versions out as the ethereum community updates it.
regularly to fix any bugs and improve it. In figure 3 it shows how the version is specified then we specify the contract and then the structure data structure is used in which the voter structure is specified which consists of weight, voted to check whether the voter has voted and vote which is the address of the delegate.

```
pragma solidity ^0.4.17;

contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        // address delegate;
    }
```

Figure 3

```
//modifer
modifier onlyOwner () {
  require(msg.sender == chairperson);
  _;
}


address public chairperson;
mapping(address => Voter) public voters;
uint[4] public proposals;
```

Figure 4

Figure 4 shows how a modifier is made to get the address of the owner that is the chairperson who will validate the eligible voter that is the only role of the chairperson the mapping of address is done with voters structure to get the address of the voters.

```
function Ballot() public {
    chairperson = msg.sender;
    voters[chairperson].weight = 2;
}

/// Give $(toVoter) the right to vote on this ballot.
/// May only be called by $(chairperson).
function register(address toVoter) public onlyOwner{
    if(voters[toVoter].weight != 0) revert();
    voters[toVoter].weight = 1;
    voters[toVoter].voted = false;
}

/// Give a single vote to proposal $(toProposal).
function vote(uint8 toProposal) public {
    Voter storage sender = voters[msg.sender];
    if (sender.voted || toProposal >= 4 || sender.weight == 0) revert();
    sender.voted = true;
    sender.vote = toProposal;
    proposals[toProposal] += sender.weight;
}
```

Figure 4

In figure 4 the function register is used by the chairperson to register the eligible voters if the weight of the voters is 0 it means the voter has already voter he/she can not vote again. We have used four candidates who have participated in the election out of which only one will win. The voters are validated using the if conditionand check if the voter is eligible and let the voter to vote for the preffered candidate.

```
function winningProposal() public constant returns (uint8 _winningProposal) {
    uint256 winningVoteCount = 0;
    for (uint8 prop = 0; prop < 4; prop++)
        if (proposals[prop] > winningVoteCount) {
            winningVoteCount = proposals[prop];
            _winningProposal = prop;
        }
}

function getCount() public constant returns (uint[4]) {
    return proposals;
}
}
```

Figure 5

Figure 5 shows the function winning Proposal returns the the winning candidate number it is done by counting the number of votes received by each candidate by using a conditional loop and check various condition and considering the candidate which maximum number of vote as the winner of the election. The election will continue until all the registered voters have not completed voting and the registeration is done on spot so it wont be a time consuming process which will let to the maximum participation of voters in the process and help in finding the rightful leader. Since there are so many checkpoints in the code it will be very difficult to manipulate the data and the data stored is immutable so the votes once casted cannot be changed which is the best feature of this process and the decentralized distributed storage provides the secure infrastructure for the whole process.

5. CONCLUSION

By building this planned sensible contract of ours, we've succeeded in moving e-voting to the blockchain platform and that we self-addressed a number of the basicproblems that bequest e-voting systems have, by victimization the facility of the Ethereum network and therefore the blockchain structure. As a results of our trials, the idea of blockchain and therefore the security methodology that it uses, specifically changeless hash chains, has become pliant to polls and elections. This accomplishment might even pave the manner for different blockchain applications that have impact on each facet of human

life. At this time, Ethereum and therefore thesensible contracts, that created one in all the foremost revolutionary breakthroughs since the blockchain itself, helped to overturn the restricted perception of blockchain as a cryptocurrency (coin), and turned it into a broader solution-base for several Internet-related problems with the fashionable world, and should alter the world use of blockchain.

E-voting remains a disputed topic inside each political and scientific circles. Despite the existence of some excellent examples, most of that ar still in use; more makes an attempt were either did not offer the protection and privacy options of a conventional election or have serious usability and quantifiability problems [7]. On the contrary, blockchain-based e -voting solutions, as well as the one we've enforced victimization the sensible contracts and therefore the Ethereum network, address (or mightaddress with relevant modifications) most of the protection issues, like privacy of voters, integrity, verification and non-repudiation of votes, and transparency of investigating. Yet, there are some properties that can't be self-addressed entirely victimization the blockchain, for instance authentication of voters (on the non-publiclevel, not on the account level) needs further mechanisms to be integrated, adore use of biometric factors.

The prominence of distributed systems stands out particularly once considering the mitigation of the danger that storing the registrations at a central location (office). this could continuously somehow enable officers to own the chance to physically access to the vote records, that could lead on to corruptions and cheatings by the authorities. in addition, in today's connected world, with the idea of the net of Things (IoT), expectedly, several non-computer devices can gain access to the net. whereas we have a tendency to ar still performing on a itinerant application as a supportive extension to our work to widen the usability; it's necessary to notice that, excluding phones and tablets; air con devices, cars, chairs, clothes, refrigerators, televisions, and lots of different everyday objects are/will be ready to directly reach to the net. In terms of blockchain, it won't be troublesome to create such distributed systems once there's such an outsized network and a reserve process power. Moreover, if of these devices work along as a grid to shorten the validation amount of transactions in a very blockchain, we'll be ready to do most of our on-line transactions firmly, reliably, and effectively, not solely in theory however conjointly in apply.

6. ACKNOWLEDGMENT

This study is a part of a broader research related to e-voting systems, and we would like to thank all who helped us a lot in completing our project work. hopefully it will help in making the voting process fair in the upcoming future.

7. REFERENCES

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: https://bitcoin.org/bitcoin.pdf .

[2] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[3] C.D. Clack, V.A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions", Mar 2017, arXiv:1608.00771.

[4] E. Maaten, "Towards remote e-voting: Estonian case", Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.

[5] U.C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: Yeni Nesil Do÷rudan Demokrasi ve Türkiye'deki Uygulanabilirli÷i", [Online]
Available: https://www.researchgate.net/profile/Umut_Cabuk/ publication/308796230_E-Democracy_The_Next_Generation_ Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408a ee7cdc685b40b/E-Democracy-The-Next-Generation-Direct-Democracy-and-Applicability-in-Turkey.pdf