ABSTRACT

Voting Dapp is e-voting systems which provided the goal of increasing security and minimizing cost. Blockchain is a major breakthrough in the technological industry that provide immense secured platform. With the launch of Ethereum, a decentralized platform which runs decentralized applications on it, a secured voting system now seems possible. There's a very high chance that a normal voting method won't lead to a clear majority. There can be many ways to deal with this issue which includes another voting process to take place which can be quite expensive in terms of time and resources. With this new vote-trading concept where the votes can be cast online. We discuss the design for the blockchain based preferential e-voting system using HTML, CSS, JavaScript at front end and truffle framework, node js, metamask, Solidity programming language where we provided one vote per candidate.

TABLE OF CONTENTS

List of Figures

CHAPTER I

INTRODUCTION

1.1 Overview

Voting system is a very crucial activity of all democratic country. The traditional voting system is leading to lot of expenditure and very un-convenient to the end-user. A whole world is exploring a secure and reliable voting system which can take care of user convenient. The advent of block chain technology has given a new hope towards the development of secure and convenient voting system.

Block chain is the public distributed database, which holds the encrypted ledger. The reason behind encrypted, is to keep the details of the user anonymous. Instead of a centralized database, all the transaction data that is shared across the nodes in the blockchain is contained in bundles of records called blocks, which are chained together to create the public ledger. This public ledger represents all the data in the blockchain. All the data in the public ledger is secured by cryptographic hashing, and validated by a consensus algorithm. Nodes on the network participate to ensure that all copies of the data distributed across the network are the same. That's one very important reason why we're building our voting application on the blockchain, because we want to ensure that our vote was counted, and that it did not change.

Since, block chain technology prevents the recorded vote from any short of tempering at the same time it offers to changes the casted option to the legitimate user. Some of the evident work done to reflect these benefits are as follows:

i. Very Vote System by Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira in which they provide the threshold encryption scheme which enable the vote and the verification without compromising the voters privacy.

ii. Securing e-voting based on blockchain in P2P network by Haibo Yi in which they provided the user credential system and compute the hash value which are based upon SHA-256. It usually used to compare the hash value to expected hash value for the Data Integrity.

iii. Secure Digital Voting System based on Blockchain Technology by Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan NED University of Engineering and Technology where they use the concept of Multichain to protect the anonymity and integrity of a vote. Their System Generate the Strong Cryptographic Hash for Each Vote Transaction based on specific user.

The user needs an account with a wallet address with some Ether, Ethereum's cryptocurrency. Once they connect to the network, they cast their vote and pay a small transaction fee to write this transaction to the blockchain. This transaction fee is called “gas”. Whenever the vote is cast, some of the nodes on the network, called miners, compete to complete this transaction. The miner who completes this transaction is awarded the Ether that we paid to vote.

Smart contracts are where all the business logic of our application lives. This is where we’ll actually code the decentralized portion our app. Smart contracts are in charge of reading and writing data to the blockchain, as well as executing business logic. Smart contacts are written in a programming language called Solidity,

The function of smart contracts on the Bock-chain is very similar to a microservice on the web. If the public ledger represents the database layer of the blockchain, then smart contracts are where all the business logic that transacts with that data lives. We’ll have a traditional front-end client that is written in HTML, CSS, and JavaScript. Instead of talking to a back-end server, this client will connect to a local Ethereum blockchain that we’ll install.

We’ll code all the business logic about our dapp in an Election smart contract with the Solidity programming language. We’ll deploy this smart contract to our local Ethereum blockchain, and allow accounts to start voting. We'll build a client-side application that will talk to our smart contract on the blockchain. This client-side application will have a table of candidates that lists each candidate's id, name, and vote count. It will have a form where we can cast a vote for our desired candidate. It also shows the account we're connected to the blockchain with under "public address" which are unique each user.

1.2 General Overview of the Problem

In a normal voting system, it usually done on paper or by electronic voting system which can lead to frauds. The money and effort for managing the voting process can be huge. The Data records can be lost and maintaining all the records can be difficult. Without the Proper Mechanism, the system can be very complex and our main aim is to provide a simple system. In a normal web application, whenever we want to access the application, we require centralized data base which is not preferable in e-voting system. By using centralized network number of votes and code for the application can be changed by any time by unauthorized user which may lead to error.

Feasibility Study

Feasibility study is an analysis that takes all of a project's relevant factor into an account including economic, technical, legal and schedule considerations to ascertain the likelihood of completing the project successfully. During the feasibility study of this projects the relevant factors were found to be feasible which is described below:

1.2.1 Economic Feasibility

There is not excess amount of cost to be spent for the completion of this project. For deployment the cost required is not much more and is affordable. therefore, after the analysis of this project was found to be economically feasible.

1.2.2 Technical Feasibility

The project can be completed on the simple systems by using node JS, metamask and Ethereum where it provides the free 10 addresses along with its private key. Not much more complex system is required for the completion of the project.

1.2.3 Legal Feasibility

As the project that is purposed will be developed within our institution using the resources available here, the legal feasibility is assured because all the software, operating system and tools available are licensed. Therefore, neither the institution nor the proposed project will face the legal threats.

CHAPTER II
LITERATURE REVIEW

2.1. Existing Systems

2.1.1. Very Vote: A Voter Verifiable Code Voting System.

Introduction

The secure platform problem of remote voting, i.e. the use of unreliable/not trustworthy client platforms such as the voter's computer and the Internet infrastructure connecting it to the election server, is one of the major problems that prevents the spread of electronic remote elections, e.g. Internet Voting. Code voting is a technique that addresses the secure platform problem establishing a secure connection between the voter and the election server by means of codes printed in a code sheet previously and anonymously delivered to the voter. This work was supported by the Portuguese Foundation for Science and Technology grants SFRH/BD/47786/2008 and PTDC/EIA/65588/2006.

Methodology:

Data were collected using a self-administered survey distributed through the internet.

Problems:

- On this system it will not show the result after voting.

2.1.2. Securing e-voting based on block chain in P2P network.

Introduction

Voting is a method to make a collective decision or express an opinion among a group or a meeting or electorates. Voting is usually following debates, discussions, and election campaigns. During voting, the person to be elected is the candidate of an election, and the person who casts a ballot for their chosen candidate is voter. Usually, the voter can vote in accordance with the list of candidate or vote for any other persons he/her prefers. The voter can submit his/her or her votes electronically to the election authorities from any location via e-voting. The election authorities are responsible for collecting votes from voters. E-voting can save time and effort with high efficiency and flexibility, which is getting more and more attentions instead of traditional voting. With the development of Internet, e-voting became the important means of many organizations. Kiayias et al. proposed an efficient E2E verifiable e-voting system without setup assumptions. Ahene et al. proposed a certificate less deniably authenticated encryption and its application to e-voting system. Kshetri and Voas proposed a blockchain-enabled e-voting system.

Methodology:

Data were collected using a self-administered survey distributed through the internet.

Problems:

- Voter’s privacy is not secure.

2.1.3. Secure Digital Voting System based on Blockchain.

Introduction

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository5 allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains.

Methodology:

Data were collected using a self-administered survey distributed through the internet.

Problems:

- The cost of ethereum gas fee is very high while casting vote.

- **CHAPTER IV**

METHODOLOGY

4.1. ARCHITECTURE DIAGRAM

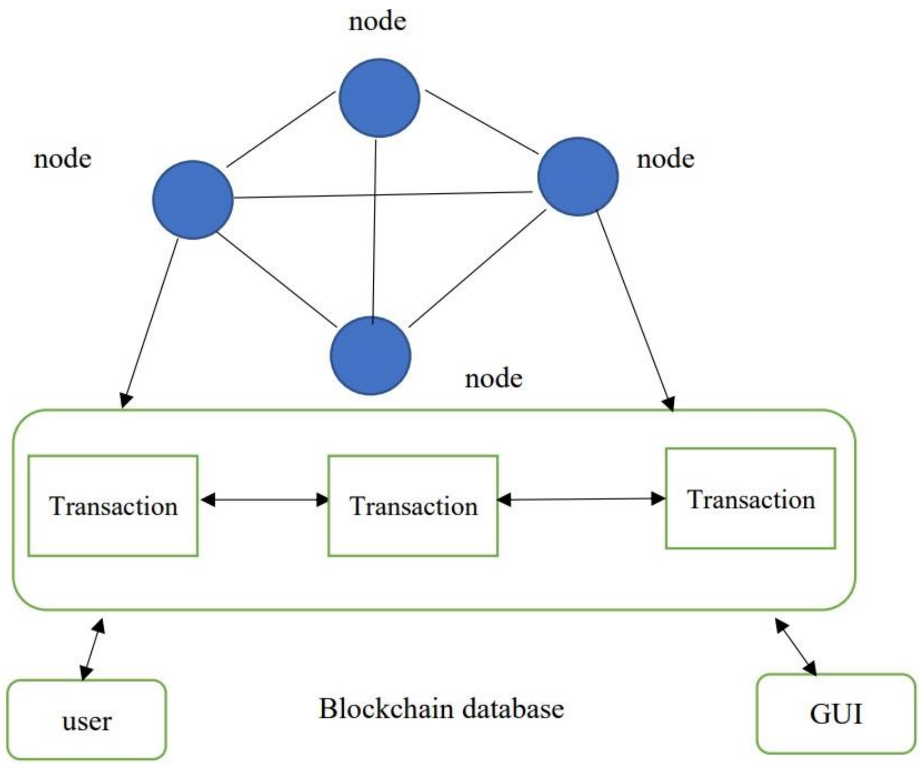

Fig-1: Architectural Diagram

CHAPTER V

RESULT AND DISCUSSION

5.1. Pseudo Codes:

Following are the pseudo codes of some of the important algorithms used in developing the application:

5.1.1 Assigning the state variable: Election.sol

Start:

```
contract Election{
//state variable
    struct Candidate{
        uint id;
        string name;
        uint voteCount;
    }
//store key value pair and read and write the state veriable
  mapping(uint => Candidate ) public candidates;
//store the candidate count cache value
    uint public candidatesCount;
    constructor () public {
addCandidate ("Ajay");
addCandidate ("Bijay");
}
}
```

End

CHAPTER VI

SUMMARY AND CONCLUSION

6.1 Summary of Achievement

By accomplishing this project, I gained a lot of knowledge about the solidity programming language and basic concept of decentralized network (Block-chain). Not only I acquire a knowledge of technical aspect but also the importance of planning and scheduling of the project. I have created simple frontend of election results where I successfully implemented and tested the contract of migration and election. It can Test the various condition at Truffle CLI where it ensure that contract code is bug free. If the contract contains any bugs, it might disable the contract and deploy the new copy. It minimizes the cost of ether during the transaction. Setup the web3 and inject the meta-mask to the local server. Each account (voters) by linking the private key at the Ethereum we can vote only one time. We can view the unique address of the account(voter) after migrating into the blockchain. Successfully incremented vote count of the candidate which lead to change in the state of the block chain.

6.4 Future scope of the project

Security and privacy are two pivotal aspects that bear the load of public expectation for evoting system using blockchain. Longer the node-chain gets it is harder for attacker to decrypt. It offers the transparency in terms of validating the accuracy of the trail of votes. Since the nodes are distributed randomly, the dependency on a centralized authority to secure the cyberspace is automatically mitigated in a Blockchain e-voting system.

6.5 Conclusion

The Block-chain technology have lot of potential to improve the traditional voting system. It is having a potential to produce a voter verifiable voting system where the voting system can be designed in a minimal cost. It can eliminate lot of effort and investment made in the traditional voting system. Therefore, the development of block chain-based voting system can be considered as very relevant in the current scenario.