Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019)
IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8

Secured voting through Blockchain technology

Teja K, Shravani MB, Chintarlapallireddy Yaswanth Simha, Manjunath R Kounte
School of Electronics and Communication Engineering,
REVA University, Bengaluru, India.
{karnamteja40, shravsmb, yaswanthsimha.cr, manjunath.kounte}@gmail.com

***Abstract*—Voting is the primary factor to change the country's future. The manual voting got replaced with the electronic machines called Electronic Voting Machines(EVM). Even after replacement, the issues continue to trouble voters. Issues like missing names in voter list, misplaced votes and so on. That is why we suggest a decentralised system to be integrated with the voting system to make it error-free. One of those decentralised systems are blockchain technology. Our project is developed on Ethereum platform using solidity language. Estonia, the blockchain country uses blockchain for almost all services. The voting procedure is presented in the paper as a case study. We summarise the tools used for the project along with its features. We also appraise the working of the our project in the further sections. Finally, we include the source smart contract code in the appendix. This project open up many possibilities to secure the voting system and help for the welfare of the nations.**

***Index Terms*—Cryptocurrency, Blockchain, Bitcoin, Decentralized, Digital signature, Cryptographic keys, D-DoS**

I. Introduction

Power and money were the primary factors driving mankind into greater heights. But when many people wanted power then the need to search for a way to select the person to be in the power increased. In those many methods, Voting is the most preferred one that most of the people in the world are used to. Voting is a process executed in a group by collective decisions for a proposal. Collective decisions are made in a different process like collecting the ballot papers, scanning for the respective candidate with the help of machines, discussion among the participants who are involved in voting, agreements among the participants. Voting provides solutions in different fields like Business, electing the CEO's, electing the president of the students union.

Voting in the political election is a process of choosing a government by giving an opportunity for electoral to elect the representatives of their government. In India, Every citizen who crossed 18 years has the right to vote. Voting provides an opportunity for the citizens to express their opinion in a nation. Voters choose their representatives on the terms like security issues, development of projects and advancements. Voting methods are of different types namely Plurality, Borda count and the hard rule. Earlier voting was done manually. Voters were supposed to put a seal on the party symbol to which they wanted to cast their vote and drop that stamped slip into the ballot box. On the voting day, government employees are appointed as election counting officers who take in charge of counting centres. These ballot boxes come to the counting centres sealed and locked. The counting officers start counting by opening the ballot boxes and separating the slips according to the parties. Vote count from all the counting centres add up and the winning candidate is who got the highest number of votes in that constituency. In this method there are many possibilities of getting errors are very high. As much of the work is done manually, the topic of trust comes into picture. This process is monitored by a centralised authority, the major single point of error may occur. And also during the counting, the trust on the counting officers should also be considered. There could a big difference in the future of that constituency even by an error of single vote. That is why we need to eliminate the manual voting system. People have come up with Electronic Voting Machines (EVM). The introduction of EVMs got a great breakthrough in India. These EVMs require no manual voting. Voters had to just press the button associated with the party they want to vote. The introduction of EVMs have helped us to overcome only the possible human errors. But the problem with the trust of centralised authority is left. That is why we introduce a decentralised system of secured voting using Blockchain technology. In voting, we also come across different issues like multiple representatives, fake voting which shows the virtual casting of the vote, hacking the voting machines, ballot shortage and so on. We need a technology to overcome the trust issue too. Blockchain technology helps in the efficient functioning and working of voting machines as it works in decentralised networks. Blockchain secures the voting system and affects all of the security issues.

II. Blockchain Technology

Blockchain is a distributed public ledger and decentralized system. Blockchain contains the sequence of Blocks which are linked through cryptography. The sequence of Blocks includes records of transactions that are immutable. Each block in the chain contains previous Block hash value and present block hash value, So it is incorruptible. Block contains two parts:

a. Block body
b. Block head

The block body has the transaction counter and transactions. Whereas, Blockhead has the following:

- Time stamp
- Previous hash value
- Nonce value
- Merkle root

Let us consider the transaction of a bitcoin between two nodes in a network. Transaction of bitcoin involves a pair of cryptographic keys namely private key and public key.

A public key of each node is accessible to everyone in the network and a private key is a secret key which makes the transaction secure and incorruptible in the network. One who wants to send the bitcoin to a node should know it's private key. Transaction of bitcoin is encrypted using private key and SHA-256 algorithm. This transaction is broadcasted in the network by the sender and it is validated by the miners. Miners play a major role in the blockchain network. They validate transactions and mine the blocks. Mining specifies the formation of a secured and valid block. A competition is held between the miners to mine the valid block, Miners get rewarded with bitcoins for mining the block in less time. A consensus is achieved with the help of proof of work algorithm. After mining the Block is agreed by other miners. If the majority agrees with the block, it is added to the longest chain in the network. Post-addition, receiver decrypts the transaction with it's private key and receives the bitcoin.

III. Voting in Estonia

E-voting or an Electronic voting system is a process of voting that use kiosks hardware systems in polling stations. This hardware system are the machines practically consists of interactional touch screen interface. With the help of this interface voters cast their ballots. E-voting gave solutions for security and accuracy issues of traditional voting. Many of the countries, tried to implement the e-voting system, but Estonia is the only country that succeeded in implementing E-voting on a large scale. E-voting in Estonia was established in 2005. Estonia includes two methods of voting system

a)Physically voting at the polling station

b)E-voting anywhere in the country.

The main aim of the Estonian government was, making the voting system easier and increase in participation of voters. The early voting system requires 3/4 of the hour to complete vote casting at the polling station, but E-voting takes 4-6 minutes to cast vote, which reduces the time to the voter. Estonian E-voting runs on Estonian ID card(E-Id cards). E-Id card provides a platform for the people and for digital signature. Voters can choose voting from home if they have a computer with an internet connection, or they can go to public libraries and university labs to cast their votes.

A. Functioning of E-voting in Estonia

Computers with internet connection allow registered voters to vote. A voter application and verification application are installed in the computers to compute the E-voting. Estonia E-voting procedure involves of following steps;

a)E-Id cards are inserted into card readers by the voters to open the web page for voting.

b)E-Id card consists of two pin codes used for specific functioning.

c) The first pin code is used to verify themselves to the central system that they are which means revealing identity.

d)A server in the central domain system checks the eligibility of the voter from the population register of the country.

e)The server displays the candidate list for the appropriate district.

f)Then the voter decides to vote for the candidate and it is encrypted.

g)Voters confirm their casting of the vote with the help of digital signature and second pin code present in the E-Id card.

h)Digital signatures of the voters will be removed during the vote count, at the last stage, the Estonia Electoral committee open the E-votes for counting where E-votes are anonymous here.

IV. Tools used for the project

A. Ethereum

Applications developed on blockchain technology are called DApps(decentralized application). Although there are many platforms to develop blockchain applications, Ethereum is preferred by the developers because it is open source and free. After the release of bitcoin ,the initial researches were carried out on the use of cyptocurrencies in different fields. Later on, the technology experts discovered the use blockchain technology in various fields other than finance.

In 2013,Ethereum was proposed by Vitalik Buterin, he was a programmer and cryptocurrency researcher. Later in 2015, it went-on live with 'premined' 72 million coins with the help of online crowd sale. At present there are more than 100 million total supply of ether.

Ethereum uses the Ether(ETH) as a built-in fundamental currency for all the transactions that happen in it. Ether is used as "gas" to run the transactions. We cannot run any of our Dapps without the minimum gas in our wallet. Ethereum has many functions over cryptocurrencies.It may be considered as an extended version of bitcoin. It broadens the scope of blockchain technology to reach out non financial applications.

Types of Ethereum accounts:

- Wallet Accounts

Wallet Accounts are general accounts created for regular transactions. Every user who wants a wallet, should register using their email-id. A seed word consisting of 12 word combination will be given to each user. It is used to recover their private keys in case if the user forgets the login password. Each wallet will be given a public key and a private key, these two keys are used for transactions.Each account will have unique address which is used to receive and send the ether.

- Smart Contract Account

These accounts are used purely for non financial purpose. Smart contract is an agreement between two or more parties where all the requisites and the conditions are written in the form of code. Each time a contract is called or executed some amount of ether is used as transaction fees. All smart contracts are deployed on a virtual machine called Ethereum virtual machine(EVM). EVM is a virtual machine that contains all required software tools to run Dapps. It allows the execution of smart contracts only if all conditions meet. For example,

pythereum is a program that use python to allow us to interact with the blockchain.

In normal cryptocurrency transactions,the amount of money to be received or to be sent is considered as data.But in smart contracts the inputs will be the data that should be hashed. Smart contracts are generally written in solidity language. Solidity is similar to many scripting languages like Java script.

B. Ganache

Ganache is a virtual blockchain that can run on any computer. Ganache provides ten accounts with 100 ether balance.This ganache is used for testing and development purposes.even mining can also be done in Ganache using advanced mining controls.

C. Truffle

Truffle is a framework developed purely for Dapp creation and development.It consists of many kinds of tools required for dApp creation. An idea converts into a Dapp comfortably using Truffle.

D. Node js

Normally java scripts are embedded into HTML codes and used on client side scripting. But Node js provides a facility of using javascript at server side too. Node js has a capacity to handle asynchronous inputs and outputs. It is designed as a event driven architecture. The paradigm "Java script everywhere" is followed by Node js. Node js is governed by the Linux foundation's collaborative projects program. All the commands and instructions are command line interfaced(CLI). We use node.js in our project for the javascripting part of the code. We use 'lite-server' as server to connect the project with chrome browser. Generally instructions start with the keyword 'npm'.

E. Metamask

Metamask is web browser extension used to manage cryptocurrency transactions. At present, the extensions are available for chrome, firefox and brave browsers. The metamask connects the normal web browser with ethereum. Each user is given a private key and public key. Public key is used as the address of the account where as private key is hidden. A 12 word mnemonic is provided as a security answer, in case where the user forgets their login password. All kinds of cruptocurrency wallets can be integrated to the metamask. So that the user can access all accounts from one place. it also has a very interactive User Interface (UI) to provide a simple and easy environment for cryptocurrency transactions.

In our project we use metamask to create, call and manage the smart contract transactions. The metamask is connected to the Ganache server and one of the ten accounts are loaded into the metamask.

V. Project implementation

A. Phases of the project

Candidate Registration:

The first registration condition to be checked for candidate registration is that the account invoking the smart contract is admin are not. The procedure continues only if the above condition is true. Only admin can add a candidate. Candidate has parameters of ID and name where as, Id is a unique parameter and name is not.

Voter Registration:

For voter registration, Voter name and address are given an input. The list of voters are kept private. For every addition of voter the variable 'voters count' gets incremented every time. For the first time registration, the variable 'voted' is given 'false' as a initial value. The variable 'registered' is given value 'True'. The variable 'CandidateId' is given value '0' as the candidate ID starts from '1'.

Self-Verification:

If voter wants to check the status of registration, they can invoke the function 'Getcurrentvoter' by providing their address as input parameter. This function returns all the details according to the the address with which it is invoked. It returns voter address, voter name, voted or not, registered or not, and if the votes had voted then it will also display the candidate id to whom the voter has been voted. This function is very useful to the voter for checking the status of their vote. If the candidate id is different than what they have voted , they can complain the admin to raise an issue.

Voting:

Vote function is the most important function in the project. The input parameters will be the candidate id to whom the voter wants to vote. The pre requisite the condition for invocation of this function is that only registered voters can only access this function. That means the variable 'Registered' should be true and also the variable 'voted' should be false. The function will first increments the vote count of the candidate whose id is provided as input then changes the 'voted' variable as 'true' and change the candidate id variable from '0' to the input candidate id. At last, it emit the event 'vote' cast with the address of the votes.

We have also included the time variable 'Time Limit' to provide the time limit to the votes. Default time will be 5 minutes . Another prerequisite for this function is the time limit. The time limit should be below 5 minutes.

Get winning candidate:

After the time limit, this function gets automatically invoked. If gives out the candidate id, candidate's name and the number of votes secured by the winning candidate. The winner calculation is done through normal array iteration method. The winner declaration will end the voting. This above explanation completes the basic smart contract execution. But to get a smooth user interface we need HTML and CSS scripts we use node js. To integrate the smart contract with the browser, we launch 'lite-server' in npm. The sequence of launching the project is,

In the project directory
1. Truffle compile
2. Truffle Migrate
3. npm run dev

Here we use metamask as wallet provider. We connect one of the ten available accounts of ganache to metamask for testing purpose .The 100 ETH present in that account is used at the development stage.

VI. Conclusion and future work

In this paper, We introduce secured voting using Blockchain technology as alternative for current existing methods. As a part of case study we have studied Estonian e-voting procedure. Estonia is a blockchain country where more than 90 percent of the services are running on blockchain technology and cryptocurrencies. A detailed study of the procedure is explained in the paper.

An idea of secured voting flashed in our minds after getting deeper knowledge in blockcahin technology's scope. Many tools had to be used to convert our idea into a Dapp. We have used ethereum as a platform to develop it. The detailed procedure along with nodes was explained deeply. Even though our project does not fit perfectly for the general political elections. It is suitable for small scale elections in associations and small towns.

Our aim is to broaden the scope of blockchain technology beyond the cryptocurrencies. It has the capability to disrupt many existing systems and technologies. We are trying to improve and implement our project for a larger scale users and to integrate the authentication and authorization checking through fingerprint verification.

Acknowledgment

The authors would like to thank Dr P Shyamaraju, Chancellor, REVA University for all the facilities provided to carry out the research activities. Also, the authors would like to thank Dr Mohammed Riyaz Ahmed and from school of ECE, REVA University for their continuous support and encouragement.

References

[1] Mukhopadhyay, Ujan, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. "A brief survey of cryptocurrency systems." In Privacy, Security and Trust (PST), 2016 14th Annual Conference on, pp. 745-752. IEEE, 2016.

[2] Pierro, Massimo Di. "What Is the Blockchain?." Computing in Science & Engineering 19, no. 5 (2017): 92-95.

[3] Bozic, Nikola, Guy Pujolle, and Stefano Secci. "A tutorial on blockchain and applications to secure network control-planes." In Smart Cloud Networks & Systems (SCNS), pp. 1-8. IEEE, 2016.

[4] Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. "Blockchain technologies: The foreseeable impact on society and industry." computer 50, no. 9 (2017): 18-28.

[5] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1-6. IEEE, 2017.

[6] Mehta, Inderpal Singh, Arnav Chakraborty, Tanupriya Choudhury, and Mukul Sharma. "Efficient approach towards bitcoin security algorithm." In Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on, pp. 807-810. IEEE, 2017.

[7] Mirzayi, Sahar, and Mohammad Mehrzad. "Bitcoin, an SWOT analysis." In Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on, pp. 205-210. IEEE, 2017.

[8] Nayak, Arpita, and Kaustubh Dutta. "Blockchain: The perfect data protection tool." In Intelligent Computing and Control (I2C2), 2017 International Conference on, pp. 1-3. IEEE, 2017.

[9] Lindman, Juho, Virpi Kristiina Tuunainen, and Matti Rossi. "Opportunities and risks of Blockchain Technologiesa research agenda." (2017).

[10] Castellanos, Alejandro, Debora Coll-Mayor, and Antonio Notholt. "Cryptocurrency as guarantees of origin: simulating a green certificate market with the ethereum blockchain." (2017).

[11] Khoury, David, Elie F. Kfoury, Ali Kassem, and Hamza Harb. "Decentralized Voting Platform Based on Ethereum Blockchain." In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1-6. IEEE, 2018.

[12] Liu, Yi, and Qi Wang. "An E-voting Protocol Based on Blockchain." IACR Cryptology ePrint Archive 2017 (2017): 1043.

[13] Yu, Bin, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. "Platform-independent secure blockchain-based voting system." In International Conference on Information Security, pp. 369-386. Springer, Cham, 2018.

[14] Chatterjee, Rishav, and Rajdeep Chatterjee. "An Overview of the Emerging Technology: Blockchain." In Computational Intelligence and Networks (CINE), 2017 3rd International Conference on, pp. 126-127. IEEE, 2017.

[15] Peck, Morgen E. "Blockchains: How they work and why they'll change the world." IEEE spectrum 54, no. 10 (2017): 26-35.

[16] Dagher, Gaby G., Praneeth Babu Marella, Matea Milojkovic, and Jordan Mohler. "BroncoVote: Secure Voting System Using Ethereums Blockchain." (2018).

[17] Eyal, Ittay. "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities." Computer 9 (2017): 38-49.

[18] Tama, Bayu Adhi, Bruno Joachim Kweka, Youngho Park, and Kyung-Hyune Rhee. "A critical review of blockchain and its current applications." In Electrical Engineering and Computer Science (ICECOS), 2017 International Conference on, pp. 109-113. IEEE, 2017.

[19] Kaushik, Akanksha, Archana Choudhary, Chinmay Ektare, Deepti Thomas, and Syed Akram. "BlockchainLiterature survey." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on, pp. 2145-2148. IEEE, 2017.

[20] eber, Ingo, Vincent Gramoli, Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, and Paul Rimba. "On availability for blockchain-based systems." In Reliable Distributed Systems (SRDS), 2017 IEEE 36th Symposium on, pp. 64-73. IEEE, 2017.

[21] Aung, Yu Nandar, and Thitinan Tantidham. "Review of Ethereum: Smart home case study." In 2017 2nd International Conference on Information Technology (INCIT), pp. 1-4. IEEE, 2017.

[22] Lee, Kibin, Joshua I. James, Tekachew G. Ejeta, and Hyoung J. Kim. "Electronic voting service using block-chain." Journal of Digital Forensics, Security and Law 11, no. 2 (2016): 8.

[23] Wst, Karl, and Arthur Gervais. "Do you need a Blockchain?." In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45-54. IEEE, 2018.