International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Ethereum Blockchain based Secure E-voting System

Sahla Sherin O, Anna Joshy, Neethu Subash

Abstract*: The security and accountability issues are a challenge to the traditional structure from still widespread elections. General e-voting system use a centralized system, where one organization manages overall system. These organisations have full control over the database and system, allowing manipulation of the database. There should be no e-voting system to secure data and potential attacks should be able to withstand. Blockchain technology should solve certain voting problems. In this paper we are implementing an ethereum blockchain based electronic voting system. Ethereum blockchain networks are used to transfer money and store data. Networks are organized by one or more machines. Every node is a machine that running an ethereum client. The eligible one can run the node. By adopting blockchain in e-voting system database distribution, one of the cheating sources of database manipulation and data loss can be reduced. This can be a better solution for the currently existing issues over rigging the electronic voting machines to win elections by the political parties in our government.

***Keywords* : Smart Contract, Blockchain, Ethereum, E-voting**

I. INTRODUCTION

Electronic voting (e-voting), designed to use electronic systems to help cast and count votes, has been the focus of cryptography work for the past few years [16]. In comparison to conventional paper-based voting, e-voting is environmentally friendly, and less prone to error. But for security reasons, e-voting system was analyzed and some flaws were identified. Due to its vulnerability and insufficient security online voting has been neglected in some countries. Because of properties like decentralization, non-repudiation, transparency, irreversibility, etc., blockchain technology can overcome potential e-voting problems [12].

Satoshi Nakamoto introduced the blockchain technology with the development of the first cryptocurrency called Bitcoin in 2008. Bitcoin blockchain technology used a decentralized distributed ledger combined with the stocastic concensus protocol based on PoW (Proof-of-Work). Because at every transaction the chain is replicated, cryptographically signed, and publicly verifiable, no-one can manipulate the data written on the blockchain. The blockchain structure is a single, appended data structure. New blocks of data can be inserted here, but cannot be modified or removed. The blocks are arranged in a way that each block includes hash of the preceding block that guarantees immutability [10].Ethereum networks consist of one, or more, nodes. Each node acts like a machine which runs an ethereum application. Blockchain follows a decentralized system, and a large number of users own the entire database. The blockchain is a database which stores a record of all transactions that have ever been made. Transaction is protected by a User Address, Private Key, and Public Key, and the created block contains the hash of all these data making data safer [12]. Through accepting blockchain in e-voting system database delivery, one of the cheating causes of data base abuse and data loss can be that. This can be a great solution to the current issues of manipulating electronic voting machines to win elections by our government's political parties. In the modern day digital technology has changed a lot in the lives of people. Unlike the e-voting system, its implementation includes several traditional uses of paper. General electoral system also uses a centralized system where the entire voting process is handled by one organization [14]. One of the problems that can occur with a centralized organization in traditional e-voting systems is that, the organization has full control over the database and system, the database can be tampered with for considerable opportunities. Blockchain technology is one approach, because it involves a decentralized system, where multiple users own the entire database. Blockchain became regarded as the decentralized system of the Bank itself. Through implementing blockchain in the e-voting systems, issues including abuse of databases can be that. The paper handles voting recording using blockchain algorithms from all polling places. Therefore transparency, verification and provability should be ensured in the voting platform. They need to ensure that the people attending the elections have genuine electoral ides and use adequate credentials in electronic environments, and should be able to prove at any time and thereby the election should be 100% clear. No-one can change the votes after they are cast. Elections need diversity, too, so nobody can vote for another. Using ethereum blockchain these can be assured by introducing e-voting. Our system provides a stable voting environment and demonstrates that the use of blockchain can provide a robust e-voting scheme. Since e-voting is open to anyone with a computer or a mobile phone, individuals and representatives will make every single administrative decision.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Sahla Sherin O*, Dept. of Computer Science and Engineering, Mar Athanasius College of Engineering, Kerala Technical University, Kerala, India. Email: sahlasherin.o.hameed@gmail.com
Anna Joshy, Dept. of Computer Science and Engineering, Mar Athanasius College of Engineering, Kerala Technical University, Kerala, India. Email: annazzzz21@gmail.com
Neethu Subash, Dept. of Computer Science and Engineering, Mar Athanasius College of Engineering, Kerala Technical University, Kerala, India. Email: neethu.subash@gmail.com

That will ultimately lead humanity to democracy. It is important to us because elections can be easily compromised or manipulated, particularly in small towns and even in bigger towns in corrupt countries. In addition, traditional large-scale elections are very costly, since hundreds of geographically distributed voting centers and millions of voters are present. In addition, voting on vacation, on a business trip or far away, which will make it impossible for that particular elector to attend the election, may also take part in the vote for any other cause.

The remainder of the paper is organized as follows. The second section presents a critical assessment of the previous work published in the research subject literature. The third section, proposed system specifies the features of the project. This section also gives the detailed design, the method of solution and architecture diagrams of the project. And finally it conclude with the relevance of the project compared to the previous work, scope for future work and states the points clearly with the original objective.

II. RELATED WORKS

The security of an election in every democracy is a matter of national security. For a decade, the computer security field has been studying the possibilities of electronic voting systems [1] with the aim of minimizing the cost of holding a national election while meeting, and increasing the security conditions of an election. The voting system was based on pen and paper from the advent of democratically elected candidates. Replacing the old pen and paper scheme with a modern electoral system is necessary to reduce bribery and make traceable and verifiable voting [2]. Electronic voting machines were deemed unreliable by the security community, largely based on physical security issues. Anyone with physical access to such machine can hack the device thus affecting all the votes cast on the above-mentioned computer. Several countries have been debating e-voting in various areas for quite some time. The leading country in the process of e-voting is Estonia, which conducted online voting from 2005 to 2007 [5]. Blockchain-based voting, on the other hand, has not yet been widely used. It is in the development process of the last few years. South Korea is a notable example that brought a successful conclusion to the 2017 Blockchain-based election [6].

In 2018, M. Pawlak [7] implemented the voting process relies on the email address of the voter which can be easily hacked or manipulated. To be sure, some individuals will always subscribe to the system using the e-mail address and voting on someone else's behalf. This method ensures none of the required qualifications like protection, data integrity or privacy that an e-voting system ought to have. In [8], P. Tarasov had suggested a peer-to-peer voting system based on blockchain. The main focus of this research is to ensure anonymity of the ballot and the blockchain vote's participation. They suggest a specific participation model for voting according to that reason. Their solution has a solid basis for such a voting commitment format, but we are proposing a different system based on another government maintained system. A further paper alongside Blockchain proposes a database solution [9]. The authors designed a system that creates blocks after electors collect ballots until the end of the election process [9] to keep them in a database. In this paper the writers have tried to eliminate the need for a database.

In 2012 Yi Liu [4] made a suggestion about a Blockchain-based e-voting protocol. The research proposed a decentralized e-voting protocol, without presence of a trusted third party. Blind signature and blockchain are the two key methods used in the protocol. The blockchain with the public key is used here. Blind signature is used during election to protect the voting choices. In comparison to ' personal use ' of blind signature, the proposal extracted a data structure from Bitcoin as 'public use' ensures clarity of the election process. In 2017 Rifa Hanifatunnisa [3] introduced a Block chain-based e-voting recording system design. In this e-voting system, a blockchain authorisation is used to render nodes the opposite of the Bitcoin system. The node in question is a place of general election, since it is necessary to register the place of election before implementation begins. This approach helps to preserve the integrity of data, which is shielded from manipulations that should not occur in the election process. The system uses Get a turn method [15].

III. METHODOLOGY

Electors will have to vote in a controlled environment to meet the e-voting privacy and security requirements, and to ensure that the electoral system does not allow for forced voting. We are setting up a public blockchain based on the Ethereum in our work to achieve these goals. Because public blockchain is more secure we use public blockchain than private blockchain. Private blockchain is a single-entity, invitational-only network. Nonetheless, public blockchain is completely transparent ledger. Because the information is decentralised, it is encrypted and stored on multiple devices. That makes a public blockchain virtually impossible to hack. A private blockchain in other hand can be altered by its owner. It is also more vulerable to hacking.

The Ethereum blockchain helps us to execute code on the internet with something called a smart contract with the Ethereum Virtual Machine (EVM) [13]. Smart contracts are software that are trackable and immutable, operating in a decentralized setting. Once the smart contract is deployed nobody can modify the code or change the behavior of its execution.Smart execution of contracts ensures binding parties to an agreement as signed. This creates a new, powerful form of trust relationship that doesn't rely on a single party. Smart contracts enable better management of digital contracts, as they are self-verified and self-executed [11]. Smart contacts are written in the programming language Solidity, which is a mix of C++ and JavaScript. Web3.js is a javascript library that allows us to use our client side application to connect to the blockchain. The block is created based on the protocol to consensus. All the network miners compete to be the first to find a solution to the mathematical problem with the candidate block. The problem can not be solved in other ways than by brute force, so that in essence a large number of attempts are needed.

When a miner finally finds the right solution, he or she simultaneously advertises it to the entire network, receiving a protocol-provided cryptocurrency prize. It is also the duty of smart contracts to audit and count the votes when the voting time is up. Our contract has functions specifying the timing and length of an election. Also any Ethereum account can be included in the elections. Since we use the account's hash values, it can not disclose the people's identity.

To make the election more secure, we want to ensure that their votes are counted and counted only once. Instead of having a network, a central server and a database, the blockchain is a network and a database in one. Through blockchain, all transaction data are stored through bundles of records called blocks, which are clustered together to construct the public ledger. All public ledger data are encrypted by cryptographic hashing, and checked by consensus algorithm.

One of the important reasons we are creating our application for blockchain voting is that we want to make sure that our vote has been counted, and that it has not changed. The user needs a wallet-address account that includes some Ether, Ethereum's cryptocurrency. When they connect to the network, they cast their vote, and pay a small transaction fee to write this transaction to the blockchain. This exchange fee is denominated' gas.' Whenever the vote is cast, other network nodes, called miners, fight for the completion of this transaction. The miner who completes this exchange will get to vote for the Ether we have paid for. Figure 1 shows our proposed system overall functioning.

MetaMask was created to make the Ethereum blockchain more accessible to the average user. A Chrome plug-in, MetaMask serves as an Ethereum plug-in which allows users to access their Ethereum wallet and connect with decentralized applications and smart contracts without running a full node. Users can use MetaMask to manage multiple accounts, and can easily switch between various networks. Since transactions are signed using the sender's private key which is stored locally on the user's computer, MetaMask can not mimic the user and send transactions on the recipient's behalf. Acting as an intermediary between the Chrome blockchain and the Ethereum, MetaMask lets users access the convenience and security of the blockchain within a popular browser.

A. Design and Implementation

In the voting transaction each voter receives the transaction ID of their vote. Using this transaction ID in our e-voting system, voters can use a blockchain explorer (MetaMask serves as the Ethereum browser) to go to an official election site and find the transaction with the corresponding transaction ID on the blockchain. Instead, on the blockchain, voters can see their votes, and verify that the votes were registered and counted correctly.This authentication process satisfies the transparency criteria, while minimizing the traceability of votes. Our proposed system is designed to use electronic Identification or passwords to authenticate the elector in order to introduce a form of secure authentication. Figure 2 describes the detailed processing.

1. The system verifies the credentials of the voter.
2. After the positive authentication, the corresponding smart contract is prompted for continued voting. Candidates are listed on smart contract. A voter may choose to do so.
3. When a candidate has been selected by a voter he or she proceeds to sign its vote.
4. When the vote is verified as valid, consensus has been reached on the particular vote. The elector receives a transaction identification of his corresponding vote.

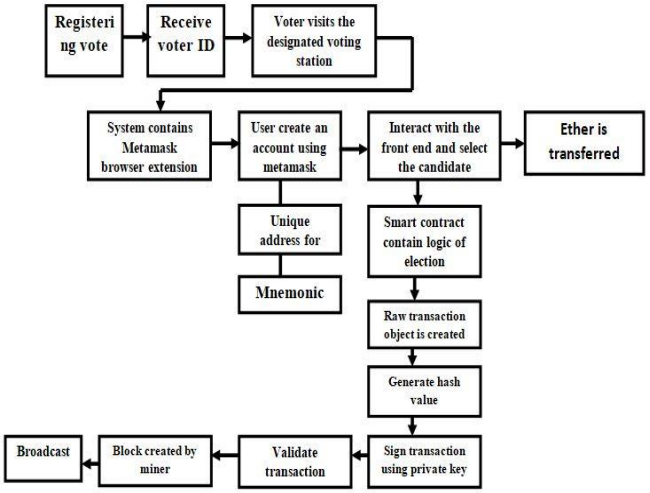

Fig. 1.Overall working of proposed system

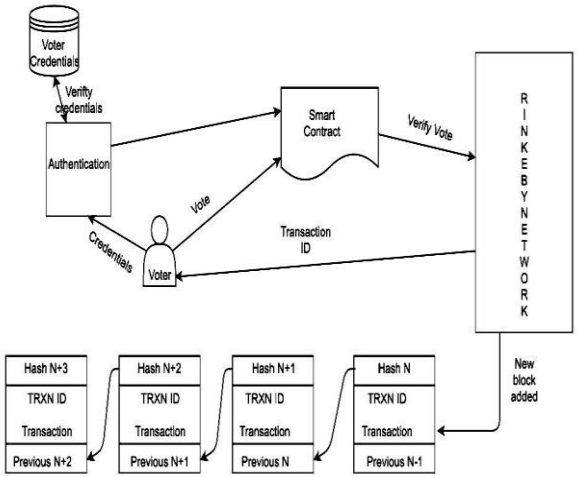

Fig. 2.Voting process

5. The vote will then be added to the block after the verification.

Use of the original Ethereum network to test experimental applications related to the development of new smart contracts is costly (because it needs some Ethers to be spent) and unnecessarily consumes enormous memory within the system. Private Ethereum networks are thus developed and made available to developers so that they can check their software without interference of the original network. One is the Rinkeby network that we used in our project as well. Fig. 3. shows a part of code of the smart contract. We have created a contract called Election, using Solidity programming. We defined Candidate as struct. The candidate id, name of candidate, vote count are initialized.

In Fig. 4. the mapping() function maps the candidate ID and the voter ID. addCandidate() function allows as to add the desired number of candidate. Fig.5. shows the code block of the smart contract which defines the verification of the vote. vote() function checks whether the voter is a legitimate voter or not. If it is a true voter the vote count will be increment else the vote will be denied.

```
contract Election {

    struct Candidate{
        uint id;
        string name;
        uint voteCount;
    }
```

Fig. 3.Code block to define structs and variables.

```
mapping(uint => Candidate) public candidates;

mapping(address => bool) public voters;

uint public candidatesCount;

event votedEvent(uint indexed _candidateId);

function Election() public {
    addCandidate("Candidate 1");
    addCandidate("Candidate 2");
    addCandidate("Candidate 3");
}
```

Fig. 4.Code block to define candidates.

```
function vote(uint _candidateId) public {
    require(!voters[msg.sender]);
    require(_candidateId > 0 && _candidateId <= candidatesCount);
    voters[msg.sender] = true;
    candidates[_candidateId].voteCount++;
    emit votedEvent(_candidateId);
}
```

Fig. 5.Code block to define verification of vote.

IV. EXPERIMENTAL RESULTS

This section provides the various results that have been obtained. On the blockchain we have developed a client-side framework that will relate to our smart contract. This client-side application will have a table of candidates listing each candidate's ID, name and number of votes. It will have a form that helps us to cast a vote for the candidate we chose. It also shows the account we're connected to the blockchain at the bottom as "your account" (Figure 6).

The back end systems must validate the vote when the voter registered the vote and thus create a block. It will record the details of the block creation as shown in Figure 7. A list that includes the number of votes for each candidate is shown after verification as shown in Figure 8.

Fig. 6.Client-side part

Fig. 7.Block creation details after voting

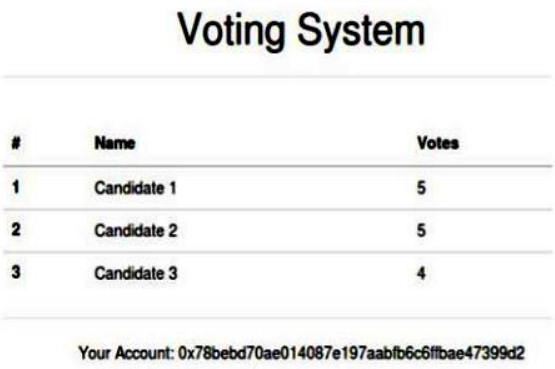

Fig. 8.Result published after voting

Developed system performance is contrasted with existing system performance. We introduced e-voting in pubic blockchains, because it is presumed that the security of such blockchains is high. It is widely believed that taking control of such blockchains is almost impossible to wield a large fraction of computing power. Alternatively, if we hold elections on a permitted blockchain, the system may be customized to meet some specific requirements. Additional programming is however needed and may result in improper design. Security flaws and functional defects may exist in private blockchain.

V. CONCLUSION

In this paper, we proposed a blockchain-based electronic voting system, which uses smart contracts to allow safe and cost-effective election while maintaining voter privacy. We also shown that blockchain technology offers new opportunities for overcoming the drawbacks and obstacles to introducing electronic voting systems. This ensures protection and dignity, and provides the foundation for accountability. We managed to move e-voting to platform Blockchain. As a result, it has become adaptable to elections with the blockchain framework. This achievement might also pave the way for other blockchain applications.

While using blockchain technology to develop an electronic voting platform, we aim to ensure that the solutions are stable and provide an electronic voting system that is secure and audited. With the project coming to an end, it can already be inferred that blockchain has the potential to improve electronic voting processes by overcoming their major limitations and problems inherently. While our developed electronic voting solution remains only a functional prototype, the experiments it undertook allow us to conclude on the feasibility of using blockchain technology in the production of these systems.

REFERENCES

1. Sos.ca.gov. (2007). Top-to-bottom Review: California Secretary of state available at: http://www.sos.ca.gov/elections/ voting-system/oversight/ top-bottom-review/
2. Nicholas Weaver. (2016). Secure the Vote Today. Available at: https://www.lawfareblog.com/ secure-vote-today.
3. Rifa Hanifatunnisa, Block chain based e-voting recording system design, IEEE 2017.
4. Yi Liu and Qi Wang, An E-voting Protocol Based on Blockchain, ISPRS Hannover Workshop 2012.
5. S. Olnes, J. Ubacht and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Government Information Quarterly, vol. 34, no.3, pp. 355-364, 2017.
6. A. Barnes, C. Brake, and T. Perry, Digital Voting with the use of Blockchain Technology, Available: https ://www.economist .com/sites/default/files/plymouth.\\pdf[Nov. 20,2018]
7. M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018.
8. M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018.
9. R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6.
10. Fridrik P. Hjalmarsson, Gunnlaugur K. Hreidarsson, Blockchain-Based E-Voting System, IEEE 2018.
11. Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized Oracle Network Available at: https://link.smartcontract.com/whitepaper.
12. K. A. M. F. M. Kirby, Votebook: A proposal for a blockchain based electronic voting system, 2016.
13. Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth.ethereum.org/.
14. R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.
15. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE 2017.
16. Fouard, L., Duclos, M., Lafourcade, P., Survey on electronic voting schemes, supported by the ANR project AVOTE 2007.

AUTHORS PROFILE

Sahla Sherin O received Bachelor of Technology in Computer Science and Engineering from MES College of Engineering, Kuttippuram in 2018 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Deep Learning, Data Mining adn Blockchain.

Anna Joshy received Bachelor of Technology in Computer Science and Engineering from Jyothi Engineering College, Cheruthuruthy in 2018 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Machine Learning, Data Mining and Blockchain.

Neethu Subash is currently working as assistant professor in the Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. She received her B-Tech Degree in 2008 and M-Tech in 2013 in Computer Science and Engineering from Mahathma Gandhi university Kerala. She has around 6 years of teaching and 2 years of industrial experience. Her research interest is in Cryptography, Image security, Blockchain and Machine Learning.