Enhanced Security on E-Voting System using Block Chain

S.Syed Nawas Husain[1], Dr.M.Mohamed Sathik [2], Dr.S.Shajun Nisha [3]
[1]*M.Phil Research Scholar, PG & Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India*
[2] *Principal & Research Coordinator, Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India*
[3]*Assistant Professor & Head, PG & Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India*

Abstract

Blockchain technology has advanced opportunities to enlarge new types of digital services. In this process of electronic voting system used in numerous countries.The election process building the democracy with in the country.In earlier systems of large assumption of Direct-Recording Electronic(DRE) for voting at polling stations around the world. Base papers on voting system which voter allow to cast vote before not verify as those voting process error.In this paper we are presented Blockchain Enabled E-voting (BEV) system using blockchain technology by using the SHA-256 algorithm and this blockchain technology based system will be authentic, elimination of human error, anonymize votes, auditable, secure and accurate and will help enlarge number of voters as well as the increased trust in their governments.

Keywords - *Blockchain, Blockchain Enabled E-voting, I voting, SHA(256).*

I. INTRODUCTION

In many of countries using electronic voting systems. National election of in Estonia adopt an first electronic voting system in this world. After Switzerland also adopt electronic voting system by Norway council election [4].Competing standard of voting systems are design good through of electronic or traditional paper ballots which number of satisfy [6]. The voters safety issuing both anonymity and preserved of guarantee against an malicious candidate from voters of cast vote.

Blockchain system: Voters sent vote through the nodes depending each node system load and then the transaction in through blockchain formation of nodes using smart contracts and the actual voting takes place in blockchain system.The smart contracts are the procedure that the nodes follow to not only verify but also add the vote in the system [5]. Each nodes are processing through the smart contract to verify the vote. The distributed network traffic system will ensure currently have node server in each state The private system of blockchain and is not approachable to the directly.

Registering to vote: The voters register to vote in process of authentication to verified through in server.All the voters details are stored in their database [5].The voters along to voting system of check personally identifiable information of voters and upload voters documentation along with an email address. Upload voters pictures and information details also verified the correct information [2]. While voting ensures anonymity and privacy before of user enters a username and password to login.

Verifying the vote: The process of verifying the vote depends on the type of election it is. Some elections allow for interim results and some do not. In either case the voter must get a confirmation that his/her transaction has been approved by the blockchain system. In case of the election that allows interim results, one of the nodes of the blockchain could be made publicly accessible. It would have a website similar to a user could enter their public key to verify whether their vote was counted [5]. This node would not have the ability to add any transactions to the system. This will be implemented through smart contracts. It will only be a reader of the transactions. This will reduce the attack surface of the system.

Counting votes: The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice [5]. The candidate with the highest amount of ether in their account wins the election. For users who abstained from voting, their ether will be sent to an Abstain Account [6]. This ensures their vote does not get misused

II. LITERATURE SURVEY

Subariah Ibrahim et al. [1] recommended socket technology and bouncy castle cryptography provider and also open source library used to provided secure communication. Privacy is guaranted by using a blind signature for voters authentication. Signature protected by using password based encryption with SHA.

Nurzhan et al. [2] implementing proof-of-concept using system amoung blockchain technology encrypted messaging streams from multi signature and anonymous and providing transaction security in decentralized smart grid energy trading without reliance on trusted third parties.

Ahmed et al. [3] recommended new electronic voting syetem design used local election for secure the number of voters has to increase as using blockchain and here registered voter ability to vote using an any device to the internet and it has mostly focused on the technical and legal issues instead of taking advantage

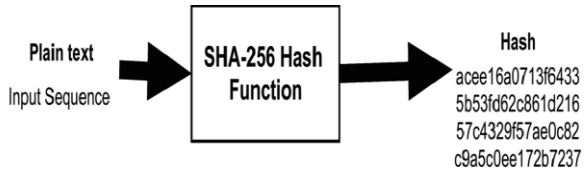
III. BLOCKCHAIN

Bitcoin is considered the first application of the Blockchain concept to create a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains blocks of transactions. Each block in the chain is linked to the previous block in the chain [7]. The first block in the chain is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain.

Table 1. Structure of the Blockchain

Field	Description	Size
Size of Block	**The size of the whole block.**	**4 bytes**
Header of Block	**Encrypted almost unique Hash.**	**80 bytes**
Transaction Counter	**The number of transactions that follow.**	**1 to 9 bytes**
Transaction	**Contains the transaction saved in the block.**	**Depends on the transaction size**

Each block in the stack is identified by a hash placed on the header. This hash is generated using the Secure Hash Algorithm (SHA-256) to generate an almost idiosyncratic fixed-size 256-bit hash [3]. The widely used algorithm was designed by the National Security Agency (NSA) in 2001 and was used as the protocol to secure all federal



communications [4]. The SHA-256 will take any size plaintext as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one-way function. The figure 1 below shows the basic logic of the SHA-256 encryption.

Figure 1. Basic Function of SHA-256 Hash

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created, which is referred to as the foundation. The primary identifier of each block is the encrypted hash in its header [3]. A digital fingerprint that was made combining two types of information: the information concerning the new block created, as well as the previous block in the chain.

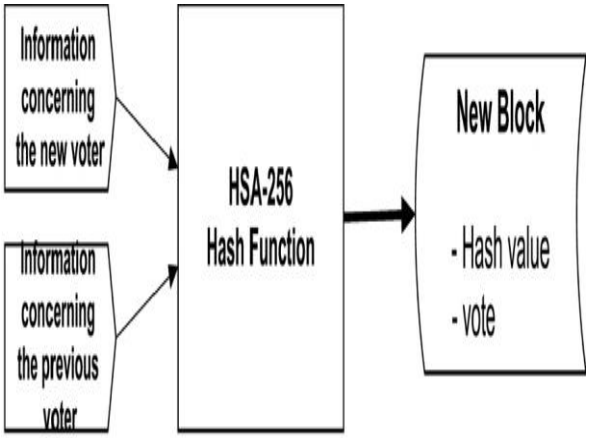


Figure 2 New Block Containing a Hash Value and Vote

A. Blockchain-based voting solutions include

E-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election [5]. Every time a person votes the transaction gets will be recorded and the Blockchain will be updated

- Transparent
- Elimination of human error
- Anonymize votes
- Faster results
- Increased trust in institutions
- Auditable
- Secure and accurate

IV. PROPOSED SYSTEM

A. System Requirements

Our e-Voting solution will include four main requirements that can be illustrated as shown below:

* **Authentication:** Only people already registered to vote can cast a vote. Our system will not support a registration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure manner [3]. Therefore, the system

should be able to verify voters' identities against a previously verified database, and then let them vote only once.

* **Anonymity:** The e-Voting system should not allow any links between voters' identities and ballots. The voter has to remain anonymous during and after the election.

* **Accuracy:** Votes must be accurate; every vote should be counted, and can't be changed, duplicated or removed.

* **Verifiability:** The system should be verifiable to make sure all votes are counted correctly. Beside the main requirement, our solution supports mobility, flexibility, and efficiency [3]. However, we will limit this paper's discussion to the four main requirements.

B. Representation of the E-Voting System

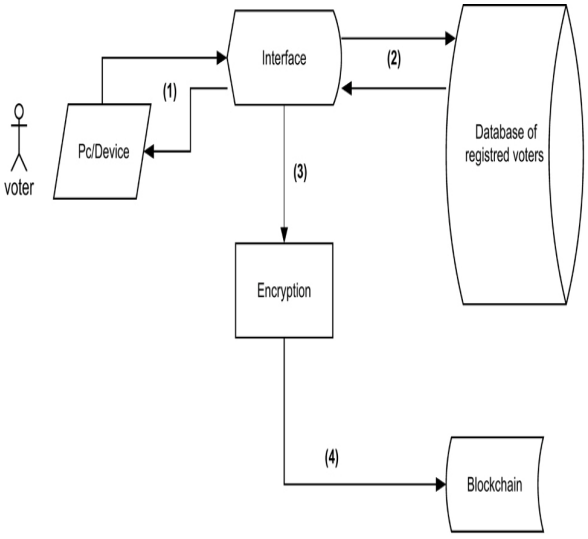


Figure 3. Simplified Representation of the e-Voting System

(1) Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-Voting system will use his Social Security Number his address, and the voting confirmation numbers provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote [3]. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

(2) Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface.

(**3) Encrypting votes:** After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of International Journal of Network each vote cast [3]. The information related to each vote will be encrypted using SHA one-way hash function that has no known reverse to it [7]. The only theoretically possible way to reverse the hash would be to guess the see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved.

(4) Adding the vote to the Blockchain: selected, the information is recorded in the corresponding Blockchain [3]. Each block gets linked to the previously cast vote.

V. CONCLUSION

We have proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it will be addressed in future research papers.

REFERENCES

[1] Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, and Shah Rizan Abdul Aziz " Secure E-Voting With Blind Signature ", 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, January 14-15, 2003.

[2] Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams " ,IEEE Transactions on Dependable and Secure Computing.

[3] Ahmed Ben Ayed, "A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM ", International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.

[4] C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).

[5] SAGAR SHAH QAISH KANCHWALA HUAIQIAN MI, "Block Chain Voting System ", https://www.economist.com/sites/default/files/northeastern.pdf

[6] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, "Blockchain-Based E-Voting System ", 11th International Conference on Cloud Computing 2018, IEEE.

[7] Rifa Hanifatunnisa and Budi Rahardjo , "Blockchain Based E-Voting Recording System Design "IEEE.