

“E-Voting Using Block Chain Technology”

Vaishnavi S. Langhe

JSPM's Bhivarabai Sawant Institute Of Technology
And Research, Wagholi, Pune – 412207
Department Of Computer Engineering

Dr. Archana Lomte

JSPM's Bhivarabai Sawant Institute Of Technology
And Research, Wagholi, Pune - 412207
Department Of Computer Engineering

ABSTRACT: Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions; because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.

KEYWORDS: *Security and Protection, Hardware, Online Information Services.*

1. INTRODUCTION

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

2. LITERATURE SURVEY

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline).Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. [1]

Bit coin introduces a revolutionary decentralized consensus mechanism. However, Bit coin-derived consensus mechanisms applied to public block chain are inadequate for the deployment scenarios of budding consortium block chain. We propose a new consensus algorithm, Proof of Vote (POV).The former guarantees the separation of voting right and executive right, which enhance the independence of bulter's role, so does the internal control system within the consortium . As for the latter, under the circumstance that at least

$N_c/2+1$ commissioners are working effectively, our analysis shows that POV can guarantee the security, transaction [2] There is no doubt that the revolutionary concept of the block-chain, which is the underlying technology behind the famous crypto currency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. [3]

Block chain was first introduced by Satoshi Nakamoto (a pseudonym) , who proposed a peer to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution. Block chain is secure by design, and an example of a system with a high byzantine failure tolerance.[4].

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment.[5]

3. PROPOSED SYSTEM

The block chain technology used mostly works the same as the block chain technology contained in the E-voting system and focuses on database recording. The nodes involved in Block chain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a block chain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in block chain creation to avoid collision and ensure that all nodes into block chain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

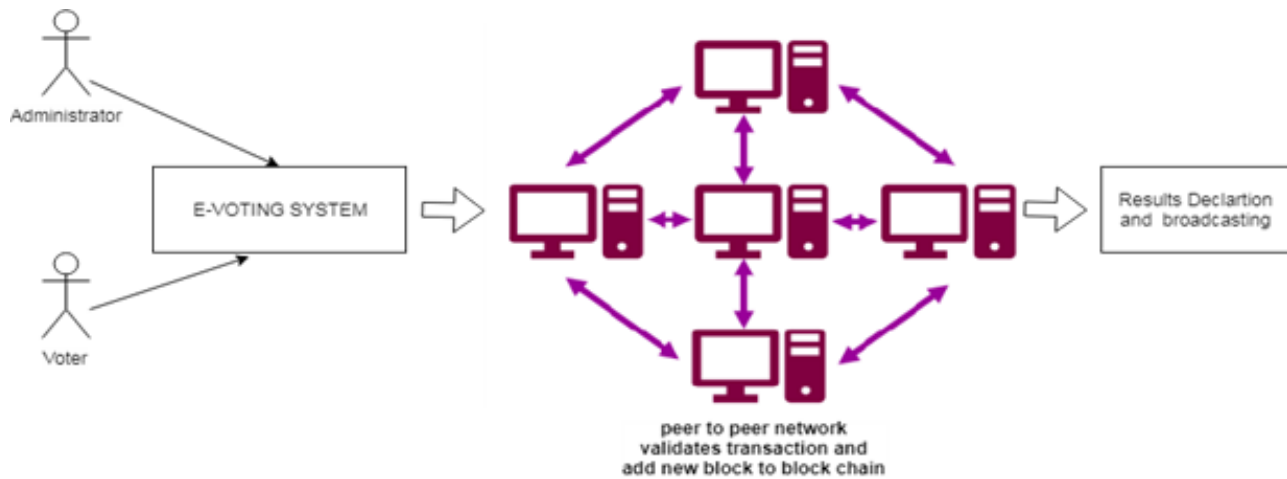


Fig. System Architecture

4. ALGORITHM

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

Such a technique thus would be lucrative for defense and security.

2 OUT OF 2 SCHEME

- Black and white image: each pixel divided in 2 sub-pixels
- Choose the next pixel; if white, then randomly choose one of the two rows for white.
- If black, then randomly choose between one of the two rows for black.
- Also we are dealing with pixels sequentially; in groups these pixels could give us a better result.

1. There is a (k, k) scheme with $m=2^{k-1}$, $a=2^{k+1}$ and $r=(2^{k-1}!)$.

We can construct a $(5, 5)$ sharing, with 16 sub pixels per secret pixel and, using the permutations of 16 sharing matrices.

1. In any (k, k) scheme, $m \geq 2^{k-1}$ and $a \leq 2^{k-1}$.

2. For any n and k , there is a (k, n) Visual Cryptography scheme with $m = \log n \cdot 2^{O(\log k)}$,
 $a = 2^{O(k)}$.

5. RESULT

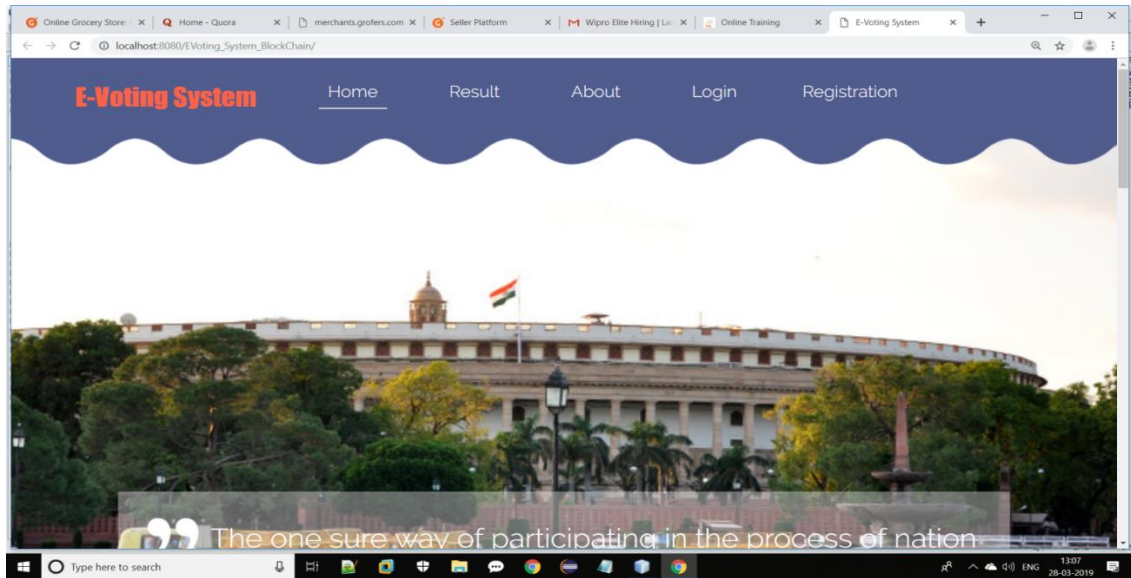


Fig: Home Page

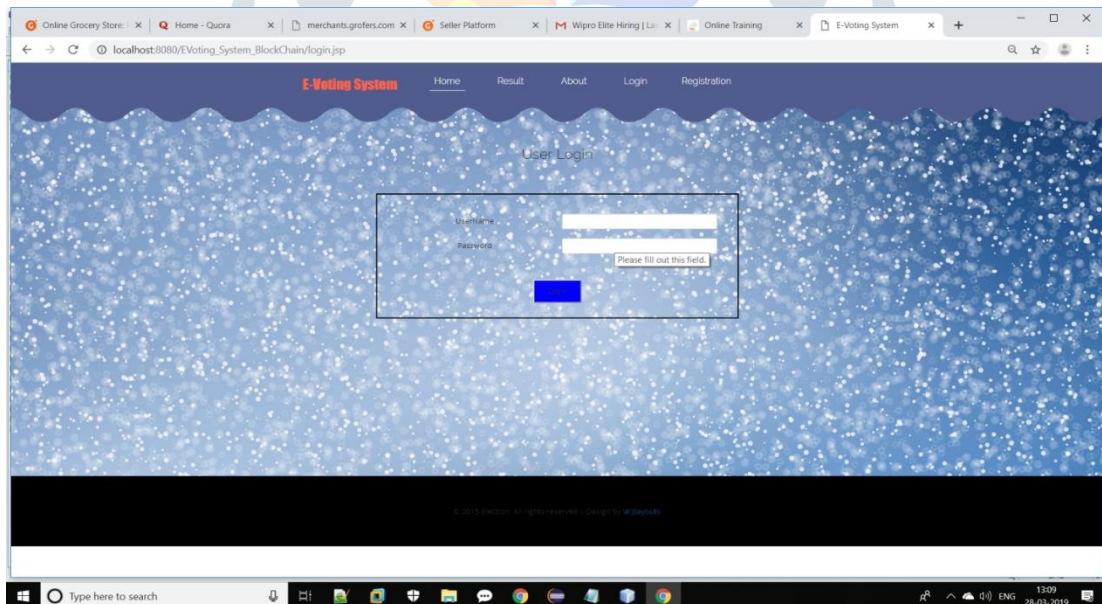


Fig: Login Page

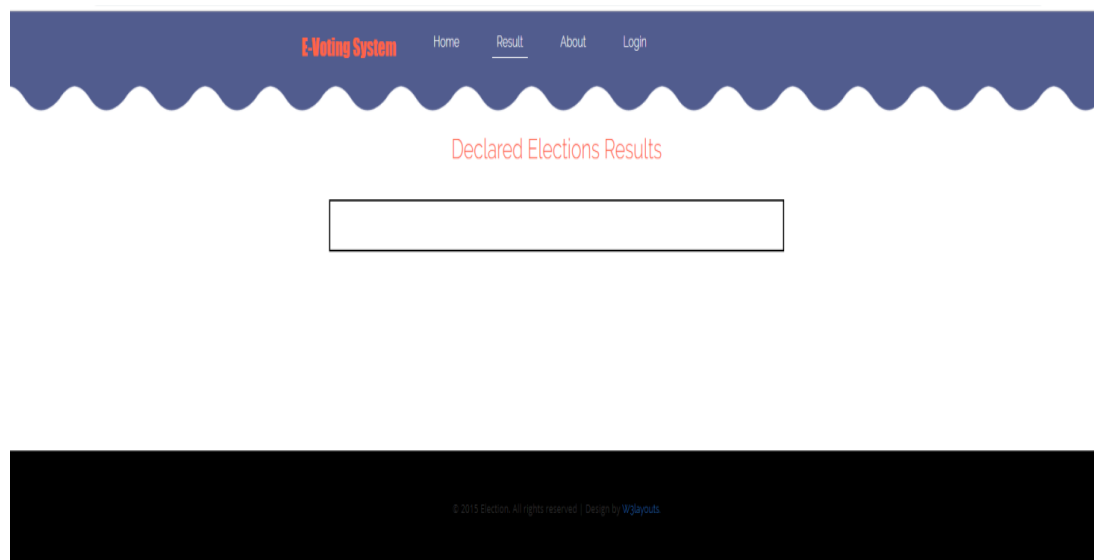


Fig: Election Result

6. APPLICATIONS

- This system is also used for corporate companies to conduct their elections for different posts such as the presidential election, manager election etc.
- Online social network
- Online banking

7. CONCLUSION

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

8. REFERENCES

1. Ahmed Ben Ayed,"A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.
2. .Rifa Hanifatunnisa, Budi Rahardjo," Blockchain Based E-Voting Recording System Design",IEEE 2017.

3. Kejiao Li, Hui Li, Hanxu Hou, Kedan Li, Yongle Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.
4. Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkilic, "Towards Secure E-Voting Using Ethereum Blockchain", 2018 IEEE.
5. Supriya Thakur Aras, Vrushali Kulkarni, "Blockchain and Its Applications – A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.
6. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", IEEE 2018, 03 July 2018.
7. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, "Secure Digital Voting System based on Blockchain Technology", IEEE 2017.
8. Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z
9. Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online] <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
10. Zyskind et. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online]. Available: : <http://dx.doi.org/10.1109/SPW.2015> Jianliang Meng, Junwei Zhang, Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.