SECURE ONLINE VOTING SYSTEMS USING BLOCK OF CHUNKS

P. Deepa[1], K. Akshaya[2], R. Priyadarshini[3], H. Saranya[4]

[1]Associate Professor, Dept.of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu
[2,3,4]U.G.Scholar, Dept.of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu

---***---

Abstract - *Distributed wireless networks perform critical network functions such as fault-tolerant data fusion, cooperative sensing, and reaching consensus in voting system . People cast their votes by going directly to voting centre or via post. However, the delay overhead of voting can be prohibitive when numerous participants have to share the post in sequence, making it impractical for time-critical applications. In this project we propose a fast and secure Blockchain voting scheme called Blockchain Voting System BVS, which significantly reduces the delay for collecting and tallying votes. In BVS, Voters transmit their votes simultaneously by exploiting the blocks in online. Votes are realized by injecting energy to pre-assigned blocks. We show that BVS is secure against hackers and third parties, that attempt to manipulate the voting outcome. Security is achieved by employing cryptography-based authentication and message integrity schemes. We analytically evaluate the voting robustness as a function of Block parameters. We extend BVS to operate in a Block groups. We discuss practical implementation challenges related to multi-device frequency and time synchronization and present a implementation of BVS. The implementation of this concept in reality can reduce the corruption in vote counting and achieve secure result in less time.*

***Key Words*: Cryptography, Blockchain, SHA, Integrity, BVS**

1. INTRODUCTION

Blockchain technology allows for fast, secure, and transparent peer-to-peer transfer of digital goods that include money and intellectual property. In crypto coin mining and investing, it's an important topic to understand. One of the most talked about and misunderstood topics in recent times, blockchain technology is completely overhauling the way digital transactions are conducted and could eventually change the way several industries conduct their daily business.

Two words that have rapidly become part of the mainstream vernacular are bitcoin and blockchain. While they are related, these terms refer to two different things. Bitcoin is a form of virtual currency, more commonly known as cryptocurrency, which is decentralized and allows users to exchange money without the need for a third-party. All bitcoin transactions are logged and made available in a public ledger to ensure their authenticity and prevent fraud. The underlying technology that facilitates these transactions and eliminates the need for an intermediary is the blockchain.

One of blockchain's main benefits lies in its transparency, as the ledger functions as a living, breathing chronicle of all peer-to-peer transactions that occur. Each time a transaction takes place, such as when one party sends bitcoin directly to another, the details of that deal — including its source, destination, and timestamp — are added to a block.

The block contains the transaction along with other similar types of transactions that have occurred recently. In the case of bitcoin transactions, the recent transactions are for the previous 10 minutes or so. Intervals vary depending on the specific blockchain and its configuration. The validity of the transactions within the cryptographically protected block is then checked and confirmed by the collective computing power of miners within the network in question.

On an individual basis, miners are computers that are configured to use their GPU or CPU cycles to solve complex mathematical problems, passing the block's data through a hashing algorithm until a solution is found. When the problems are solved, the block and all of its respective transactions are verified as legitimate. Rewards — bitcoin or some other currency — are then divvied up among the computer or computers that contributed to the successful hash.

When the transactions within a block are deemed valid, they are attached to the most recently verified block in the chain, creating a sequential ledger which is viewable by anyone.

This process continues in perpetuity, expanding on the blockchain's contents and providing a public record that can be trusted. In addition to being constantly updated, the chain and all of its blocks are distributed across the network to a large number of machines. This ensures that the latest version of this decentralized ledger exists virtually everywhere, making it almost impossible to forge.

2. LITERATURE SURVEY

[1] Secure Physical Layer Voting, by Bocan Hu,Yan Zhang,Nirnimesh Ghose and Loukas Lazos Distributed wireless networks perform critical network functions such as fault-tolerant data fusion, cooperative sensing, and reaching consensus in voting system. They use

fusion centre for sending messages which is less secure and a slow process.

[2] Extreme automation is the latest initiative to have emerged from several "hands-free". Innovations like autonomous Ships and submarines, autonomous passenger aircraft, drone freight delivery, autonomous robotic surgery, automated knowledge discovery while the healthcare industry will need to adapt to the changing care delivery model as it will save many billions of dollars.

[3] A large portion of the population in the developing world can benefit from blockchain technologies. It can be argued that in many ways, blockchain has a much higher value proposition for the developing world than for the developed world but people suffer from inefficiency, fraud, and gross misallocations of resources.

[4] Blockchain is a technology that uses community validation to keep synchronized the content of ledgers replicated across multiple users. Although blockchain derives its origins from technologies introduced decades ago, it has gained popularity with Bitcoin. Bitcoin's blockchain is a decentralized peer-validated time-stamped ledger that chronologically registers all valid transactions. It is a slow operation with limited governance.

[5] Blockchain and the Internet of Things (IoT) are key technologies that will have a huge impact in the next 10 years for companies in the industrial market. This article describes how these two technologies will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility. Third-party repair partners could monitor the blockchain for preventive maintenance and record their work on the blockchain.

3. EXISTING SYSTEM

Voting is done by people through voting booth or via post. However, the delay overhead of voting can be prohibitive when numerous participants have to share the post in sequence, making it impractical for time-critical applications.

The vote counting had major issues like corruption and slow progress

3.1 Disadvantages

- Slow process
- More possibilities for Corruption
- Low security

4. PROPOSED SYSTEM

We propose a fast and secure Blockchain voting scheme called Blockchain Voting System BVS, which significantly reduces the delay for collecting and tallying votes.

In BVS, Voters transmit their votes simultaneously by exploiting the blocks in online. Votes are realized by injecting energy to pre-assigned blocks.

We show that BVS is secure against hackers and third parties, that attempt to manipulate the voting outcome. Security is achieved by employing cryptography-based authentication and message integrity schemes.

4.1 Advantages

- Blockchain give more security in decentralised network.
- Results comes transparently and simultaneously.
- Hacking possibility is very low against the Blockchain and cryptography.

4.2 System Architecture

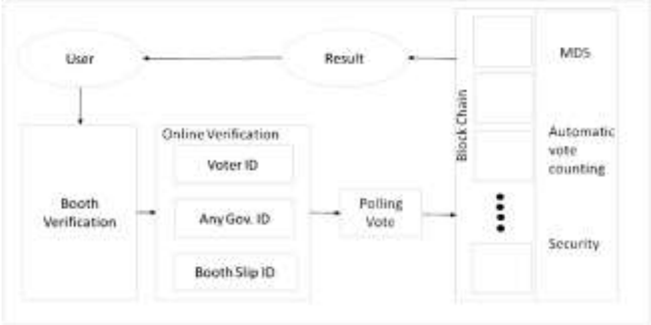

Fig -1:System Architecture

4.3 System Modules

Block chain

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. "Picture a spread sheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain. Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

Identity Management

Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. Identity management (IdM) is the task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, and information that describes information and actions they are authorized to access and/or perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified. Managed entities typically include users, hardware and network resources and even applications.

Online Voting System

The Online Voting process is in need of a standard and secure electronic system that voters can rely on and have trust in. Currently, each state implements its own process for voting; the lack of consistency between polls results in numerous problems. Various models have been developed to address the issues of security, privacy, validation, and quality control. However, these models do not meet all of the requirements needed for a good system. Exploring online voting from a systems perspective can demonstrate the commonalities of the current systems and the possible

Algorithm Used

SHA-256
Overview
SHA-256 operates in the manner of MD4,MD5 and SHA-1.The message is to be hashed first.

[1] Padded with its length in such a way that the result is multiple of 512 bits long

[2] Then parsed into 512-bit message blocks M^1 ,M^2,M^3,………,M^n
The message blocks are processed one at a time:Beginning with a fixed initial hash value $H^{(0)}$,sequentially compute
$H^i=H^{(i-1)}+C_M^{(i)}(H^{(i-1)})$,
Where C is the SHA-256 compression function and + means word wise mod 2^{32} addition.$H^{(N)}$
Is the hash of M.

Steps

Step 1: Pad the message in the usual way.i.e.Append the bit "1" to the end of the message ,and then k zero bits,where k is the smallest non-negative solution to the equation l+1+k=448 mod512.To this append 64-bit block which is equal to the number l written in binary.

Step 2:Parse the message into N 512-bit blocks M^1,M^2,M^3,……M^n.The first 32 bits of message block I are denoted M_0^i,the next 32 bits are M_1^i,and so on upto M_{15}^i.We use the big-endian convention throughout,so within each 32-bit word,the left-most bit is stored in the most significant bit position.

Step 3:The hash computation proceeds as follows:
For i=1 to N (N=number of blocks in padded message)
{

- Initialize registers with (i-1)st intermediate hash value.
- Apply the SHA-256 compression function to update registers.
- Compute the ith intermediate hash value H^i.

$H_1^i=a+H_1^{i-1}$

.

.

.

$H_8^i=h+H_8^{i-1}$

$H^{N=}H_1^N,H_2^N,….,H_8^N$ is the hash of M.

5. IMPLEMENTATION RESULTS

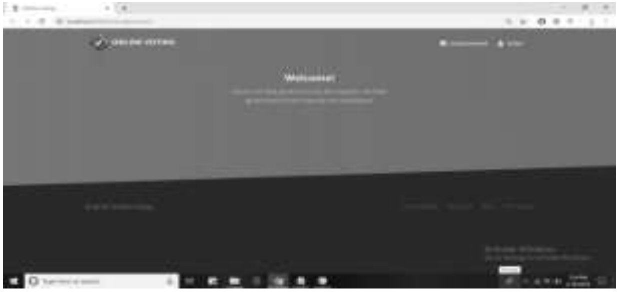

Fig -2: Home Page

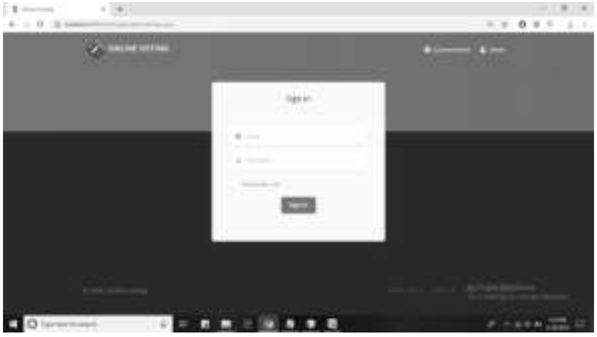

Fig -3: Government Login

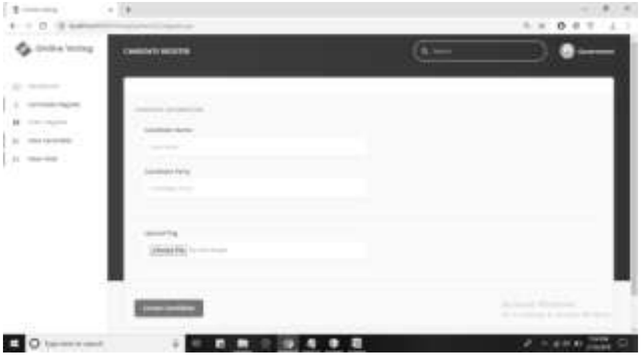

Fig -4: Candidate Register

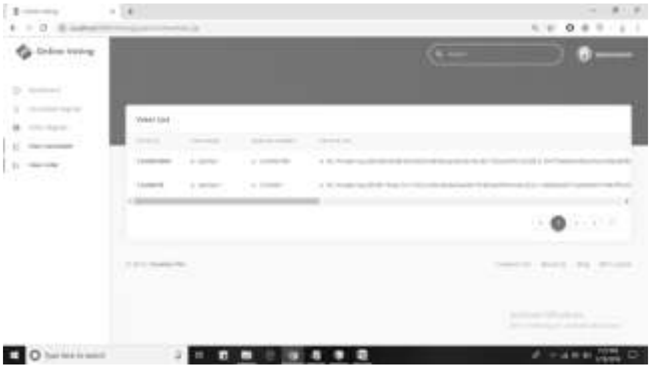

Fig -5: Candidate List

6. CONCLUSION

Our Online-Voting System is secure because user can only vote by entering CNIC. No other information is shown to the user on the polling interface. On the other hand ADMIN has the only rights to check and count all votes and announce the final result. Although there are many voting apps for this purpose but their security level is not up to that mark.

REFERENCES

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. Physical Comm., 4(1):40– 62, 2011.

[2] N. Al-Nakhala, R. Riley, and T. Elfouly. Distributed algorithms in wireless sensor networks: an approach for applying binary consensus in a real testbed. Comp. Nets., 2015.

[3] J. G. Andrews, A. Ghosh, and R. Muhamed. Fundamentals of WiMAX: understanding broadband wireless networking. Pearson Education, 2007.

[4] D. Barbara and H. Garcia-Molina. The reliability of voting mechanisms. IEEE Trans. Computers, 36(10):1197–1208, 1987.

[5] M. Barborak, A. Dahbura, and M. Malek. The consensus problem in fault-tolerant computing. ACM Comp. Surveys, 25(2):171–220, 1993.

[6] D. Bharadia, E. McMilin, and S. Katti. Full duplex radios. In Proc. of the SIGCOMM Computer Communication Review, pages 375–386. ACM, 2013.

[7] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava. Integrity codes: Message integrity protection and authentication over insecure channels. Dependable and Secure Computing, IEEE Transactions on, 5(4):208–223, 2008.

[8] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson. Distributed eventtriggered control for multi-agent systems. IEEE Trans. on Aut. Cntrl., 57(5):1291–1297, 2012.

[9] A . Dutta, D. Saha, D. Grunwald and D.Sicker.

SMACK: aSMARTACKnowledgement scheme for broadcast messages in wireless networks.ACM SIGCOMM Comp.Comm.Rev.,39(4):15-26,2009.