

Security Enhancement of EVM using Blockchain Technology

Prince Kurian¹

¹ Assistant Professor, Information Technology Department, Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India

ABSTRACT

Now a days a lot of money has been spent for conducting voting. Previously voting has been done using physical paper wallet. Now it is changed to electronic Voting Machine. But cost of conducting voting with these methods is too high and it is required large human efforts also. In addition to human efforts it is required to setup polling booth with high security, to conduct voting. Another burden with traditional systems is booth hijacking and unauthorized voting. Also all voters has to go the polling booth and they may wait in the queue for long time. The system is so costly, time consuming and requires a lot of human efforts. To avoid all such problems we can implement EVMs based on blockchain technology. The main advantage of the proposed system based on blockchain technology is no one can alter any data in the system. No human interaction is required and system itself is secure. If anyone hijacked any EVM machine also makes no issues in the system, because it uses blockchain technology

Keyword - EVM, blockchain, security

Introduction

In the traditional way of voting system is ,Initially setting up a highly secure booth with some EVMs and so many officials has to do many more prework to conduct the voting. Even though we setting all this, there may be have some problems like hijacking booth and some unauthenticated people's voting etc .Also citizen facing some problem that they may have to travel their polling booth and may have to wait for long time to do the voting. They are not permitted to do their polling any other place except some pre assigned polling booth. To avoid all such difficulties we can use blockchain technology in the EVM machine. In this proposed system we can setting up our EVM at any public place (like ATM's) like Bus stand, Railway station etc.The citizens who wants to vote, has to visit any of this place and they can poll their vote.

How it Works?

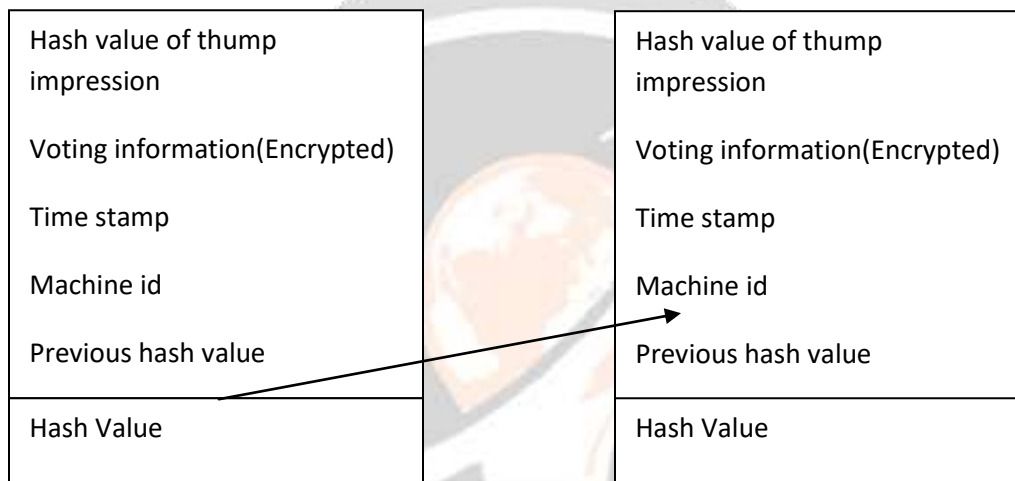
If an one wants to poll his vote ,has to drive near by EVM machine centre and by using his thump impression he can open the door .In side the room EVM is set up, he can again activate the EVM using his thump impression .After valid thump impression is identified it will display all competents photo with election symbol. He can press one any one of them and leave the room. That is process of voting in concern with normal citizens. The system worked with thump impression reading so that no one except the authorized voter can make use of his voting.

When a person mark his voting, that voting information is stored in a block and ,it will be added to a blockchain. And this blockchain is distributed among all the EVM's. This EVM's are connected through a separate network to ensure the security .When a person enters his vote a new block has been created with following informations.

- 1.Hash value of his thump impression
- 2.Ecrypted value of voting information

3. Time stamp
4. EVM id
5. Previous hash value
6. hash value of above 5 items

After creating a new block with these items it will be added to the existing blockchain. After adding this block in the blockchain his voting process will complete and next person can use this EVM. When a blockchain is updated by adding a block with above informations, this blockchain will be distributed to all other EVM. If any of the EVM get crashed or someone hijacked means, it won't affect the process. Because valid blockchain with all valid voting information available in all the EVMs.



The above figure shows a valid blockchain with 2 blocks. That means persons already voted from his location. And these blocks added to the blockchain. This blockchain is distributed among all the EVM's.

What are common issues and how this system solves the problems?

1. Unauthorized voting:

In this system we are using voters thump impression to validate the voter instead of human election card verification. So only authorized person can poll his vote.

2. Booth hijacking:

If anyone tries to steal the EVM, it won't affect the process. Because valid blockchain is distributed among all the EVMs. If any one of the EVM is available then we can retrieve all the data. And hijack all the EVM's is practically impossible.

3. Tries to do his own EVM in the network

It is impossible to connect his own machine in the network. Because pre installed EVM in the network has given some id. If any one polls his vote the new block created with that valid EVM id. So fake machines can easily be get detected.

4.Hacking and altering data:

As this system is based on blockchain technology the system is unhackable. If anyone tries to alter any data in the block, it can easily get detected because altering data causes automatically changing the hash value in the block, but the original hash value is stored in the next block also. If anyone wants alter the data, he needs to alter all blocks in the blockchain. This is practically impossible .If he alter all blocks then also we can identify that modification because valid blockchain is stored all the EVM's. So hacking is impossible

5. Threatening:

This proposed system provides high confidentiality, so that no one can read to whom the voters vote gone.

6. Malpractices:

We can avoid all type of malpractice through this system. Only valid voter can poll his vote successfully. Because we are using his thump impression to activate the machine. Once his voting done no one can vote using his id because his voting information is already added to the blockchann.

Advantages:

In this proposed voting system we can use only thump impression to validate the user. The need not carry all type of id proof documents with him. Also voter need not go to the specific EVM, he can do his voting at any locations. Since it uses blockchain technology security is ery high. Also cost of implementation is very low since this system itself ensures security. No human officials service needed. So we can reduce the cost of polling. Since there is no precertification the voter can complete his voting process within seconds. So this method is very cheap, secure and time saving

Conclusion:

In this proposed system we are using blockchain technology to ensure confidentiality, authentication and security. This method is very cheap and highly secure. Also this method is very helpful during the counting process. We can announce the results within seconds .The entire process requires no human efforts so that errors may be very less and security is very high. Once this system is established we can use the same system for later years. So only cost arise during the initial set up. If we adopt this system it will surely increase the polling percentage because voter can poll his vote at any location.

References:

1. www.edureka.co/blog/blockchain-tutorial [Accessed on 18-Dec-2017]
2. <https://en.wikipedia.org/wiki/Bitcoin> [Accessed on 18-Dec-2017]
3. <https://bitcoin.org/en/> [Accessed on 18-Dec-2017]
4. Reid F, Harrigan M, "An Analysis of Anonymity in the Bitcoin System",2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT), Boston, MA, USA , 9-11 Oct. 2011.
5. Karame G, Androulaki E, Capkun S, "Double-Spending Fast Payments in Bitcoin", Proceedings of ACM CCS 2012.