Blockchain Based Electronic Voting System

Mohammad Rasheed Ahmed
Department of Electronics and Communication Engineering
IIIT Naya Raipur
Chhattisgarh,India
rasheed1701@iiitnr.edu.in

Shivam Gupta
Department of Electronics and Communication Engineering
IIIT Naya Raipur
Chhattisgarh, India
shivamg1701@iiitnr.edu.in

Ashwini Kumar
Department of Electronics and Communication Engineering
IIIT Naya Raipur
Chhattisgarh, India
ashwini17101@iiitnr.edu.in

Dr.Ruhul Amin
Department of Computer Science and Engineering
IIIT Naya Raipur
Chhattisgarh, India
ruhul@iiitnr.edu.in

***Abstract*—It has been a challenge from long time for an electronic voting system that proves to satisfy all the legal requirements of voting. Decentralised technologies has been compelling technological advancement in the information technology world. Blockchain technologies is based on distributed ledger system and offers innumerable applications with features like immutibility etc., benefiting sharing economies. This paper focuses to asses the use of blockchain as a service to implement electronic voting systems. The paper identifies the limitations,both technological and legal, of the current voting system and briefs how realizing such system with using blockchain can be benificial. Through the description of proposed architecture, the process of an election and implementing a blockchain-based system the paper explains how the security is improved and how the limitations can be overcome.**

***Index Terms*—blockchain, distributed ledger, decentralised, electronic voting system, immutability**

I. Introduction

A. Blockchain Technology

Blockchain is a distributed ledger system. It functions as decentralized database system over distributed peer to peer network, in which each node has same ledger and all the copies are updated simultaneously in the network.Figure 1.1 shows the network model of blockchain which uses mesh topology. Literally blockchain is chain of blocks but in the traditional sense of words. When we say block and chain we mean, in this context, the digital information (the block) and the database(the chain). Basically a block contains three parts hash, previous hash and information.

B. How does Blockchain works?

A user requests for a transaction. A block representing the transaction is created. The block is broadcasted to all the nodes of the network. All the nodes validate the block and the transaction. The block is added to the chain. The transaction gets verified and gets executed.

There are basically two types of blockchain. 1. Private Blockchain 2. Public Blockchain. Public blockchain is an open network where anyone is free to join the network whereas a private blockchain is permissioned network which places restrictions on who are all allowed to participate in the network.

C. Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.digital signature-it is electronic verification of the sender. Digital signature serves three purposes 1.Authentication-give reason to believe that the message was created and sent by the claimed sender. 2.Non-repudiation-sender cannot deny having sent the message later on. 3.Integrity-ensures the message was not altered in transit. Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

D. SHA 256

SHA-256 stands for Secure Hash Algorithm 256 bit and is a type of hash function commonly used in Blockchain. A hash function is a type of mathematical function which turns data into a alphanumeric string called a hash. Developed by National Security Agency(NSA) its an algorithm which takes a input or message and it returns fixed size alphanumeric string. It doesn't matter how big is the input is output will always have fixed 256 bit length. It preserves the integrity of any amount of data.

E. RSA

RSA (Rivest Shamir Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. To understand Asymmetric, two different keys need to understood. First one is public key, the name is so because it can be given to anyone in the network. The other key is private key. The sender encrypts

message using data and private key and the receiver uses sender's public key and data to decrypt. It is also a key pair (public and private key) generator. In the proposed model we use RSA algorithm for digital signature.

II. ISSUES WITH THE CURRENT VOTING SYSTEM

The paper attempts to address certain issues with current voting system.In the paper Electronic Voting Machine is abbreviated as EVM.

A. Electronic Voting Machine Sealing Process

The current Electronic Voting Machines are loosely protected. Election officials use seals on various parts of machine. "Fig. 2" shows the images of Electronic Voting Machine sealing process. These seals are easy to tamper with. Most of these consists of stickers or red was. Scientists really don't know how to make seals that cannot be cheaply faked or tampered with. Even at nuclear facilities this is the case. This waxes are extremely weak defence.

B. Memory Manipulation

The votes can be changed while machines stored in strong room between the elections and the public counting session. Small vote stealing tools which can clipped directly onto the memory can be built. The dial on the device can be used to change the vote. This is shown in "Fig. 1"

C. Duplicate Votes

It is quite often that some may voters may not come to cast their vote. This raises the issue of duplicate votes. If the identity verifying officer at the polling booth is bribed, then it becomes quite easy to cast others vote.

III. PROPOSED ARCHITECTURE

A. Proposed Election Procedure

In this proposed model, we use private blockchain over a constituency (Member Legislative assembly elections) or over a district (Member of parliament elections). The main idea is to implement a private blockchain where each node is an EVM. In the following subsections, we will understand the roles and components for implementing the proposed idea for voting. We begin by explaining the election key components followed by election process and in the last section we will discuss design and implementation.

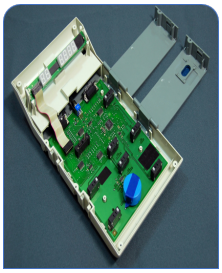
B. Elections Key Components

The proposed model has components with different roles. The roles of components in the proposed model are following:

(i) Constituency and District Nodes
Each polling station has two EVMs, one for the MLA elections and one for MP elections.

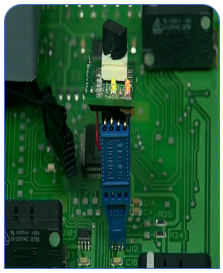
(ii) Boot Nodes
A general node that is used to ease the process of connecting the nodes.With permissioned access to the network a bootnode is hosted. A bootnode helps the district nodes to discover each other and communicate. The bootnodes do not keep any state of the Blockchain and is ran on a static IP so that district nodes find its peers faster. Two bootnodes are hosted in our proposed model ,one is for MLA election nodes and one is MP election nodes.

(iii) Fingerprint Devices
The biometric verification can be used to verify whether a voter has voted previously .This is done at inside the EVM. Any duplicate voter found will not able to cast his vote.



(a) Hardware of Electronic Voting Machine

(b) Device that can clipped to EVM memory



(c) The dial can be used to change the votes

Fig. 1: Tools used for Tampering EVM

C. Election Process

The following are the main activities in the election process:

(i) Connecting the nodes over a peer to peer network
Before the election process begins all the EVMs need to be connected to each other in a peer to peer network. To do this a bootnode is hosted first and all the EVMs are connected. Once all nodes are up, we can begin the election process.

(ii) Biometric Verification
A voter had to undergo biometric verification before casting his vote. Every block has hash which is generated from voters fingerprint .The generated hash iterated over entire blockchain and in every iteration ,hash is matched with all the fingerprint hash values in each block . As each fingerprint is unique each hash generated will be unique. Once the voter is verified then he is allowed to vote.

(iii) Validation at the receiving node
At the receiving node all the blocks are authenticated

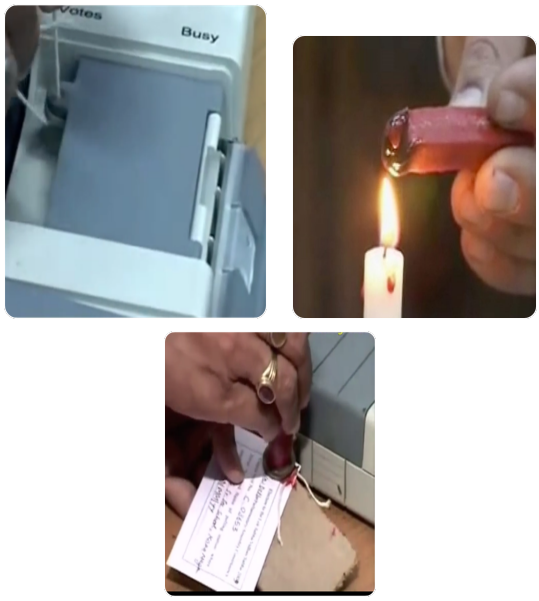


Fig. 2: Images showing EVM sealing process

using the digital signature. Any change in the data of block during transmission will result in a different signature at the receiving node, making the block invalid.

(iv) Counting and Results
The votes are calculated from the blocks. The counting will take place at every node and so can be seen at node itself. The conventional counting button present in the current system is used.

IV. IMPLEMENTATION OF THE PROPOSED SYSTEM

A. The Block

The block has the following fields

(i) Index: Index indicates the block number of the block.
(ii) Previous hash: The previous hash is the hash of the previous block.
(iii) EVM-ID: It is the unique identification number for EVMs.
(iv) Choice: The value in choice field represents a candidate or a party.
(v) Choice: The value in choice field represents a candidate or a party.
(vi) Signature: It is the hash value used for validating a block.
(vii) Fingerprint hash: It is the hash of the fingerprint of voter.
(viii) Time stamp: The date and time of creation of block.

B. Block Creation

A block is generated only after the hash of voters fingerprint is matched with all the blocks in the chain. If hash matches with none of the blocks then a new block is generated with the data.

C. Fingerprint Hash

SHA 256 hash is generated from fingerprint collected. The hash so obtained is converted to SHA 128 hash. This done to reduce the space and increase security. So double hashing is done.

D. Consensus Mechanism

This consensus is achieved using digital signatures. For authentication of blocks we propose RSA algorithm for digital signature. The private key along with choice, fingerprint hash and EVM id are used to generate to signature at the node where vote is casted. At all other EVMs using the public key along with fingerprint hash, EVM id and choice the signature is verified. All authenticated blocks are deployed onto the blockchain.

E. Smart Contract

A smart contract includes identifying the roles that are involved in the agreement and the different transactions and components in the process.

(i) Election officials: Manage the life cycle of an election. The election officials specify the election type and create aforementioned election, configure EVMs, decide the lifetime of the election and assign permissioned nodes.
(ii) Voters: For elections to which they are eligible for, voters can authenticate themselves through biometric, cast their vote and verify their vote after an election is over.
(iii) Constituency nodes: When election official creates an election, each node on network representing EVM Are deployed onto blockchain. When an individual cast their vote. Vote converted into block and broadcasted to all other nodes on network, After each node verified the block through digital signature and biometric hash then it gets added on blockchain.
(iv) Vote transaction: when an individual votes at voting district its vote recorded in block which get signed

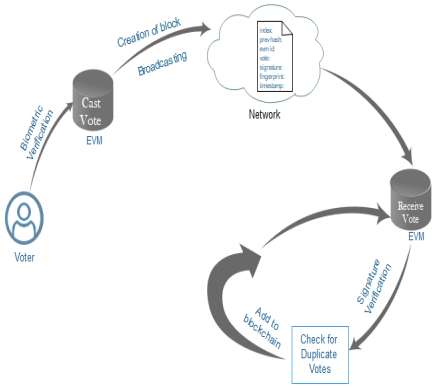


Fig. 3: Proposed Architecture

by EVM node and then broadcasted to other EVM nodes on network which then appended to blockchain after the concensus reached i.e, digital signature get verified and biometric hash doesnt matched to other blocks in Blockchain. Each vote is a block transaction on blockchain, each block holds EVM id, vote , digital signature, biometric hash. Biometric is checked every-time block needs to be added, not enabling voter to vote again.

(v) Tallying results: Results can be announced as soon as election get over through iterating on blockchain, any tampering with vote data can be detected using blockchain property.

F. Counting

The votes are counted by iterating over the blockchain. Inside the EVM during the counting process, the counter for each candidate is increased whenever a vote is found for the particular candidate. The proposed architecture is shown in "Fig. 3".

REFERENCES

[1] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, Ningxiao Lu, "Large-scale Election Based On Blockchain,"*2017 International Conference On Identification,Information And Knowledge in The Internet Of Things,*vol. 129,pp. 234-237, April, 2018.

[2] PierreNoizat,*Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data*,Academic Press,pp.453-461,May 2015.

[3] Fririk . Hjlmarsson, Gunnlaugur K. Hreiarsson, "Blockchain-Based E-Voting System," *in Proceedings of2018 IEEE 11th International Conference on Cloud Computing (CLOUD),*San Fransisco, July 2018.

[4] Rifa Hanifatunnisa, Budi Rahardjo , "Blockchain based e-voting recording system design,"*in the Proceedings of 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA),* Lombok, Indonesia, Feb. 2018.

[5] Teogenes Moura, Teogenes Moura, "Blockchain Voting and its effects on Election Transparency and Voter Confidence,"*Proceedings of the 18th Annual International Conference on Digital Government Research,* pp 574-575, Staten Island, NY, USA ,June 07 - 09, 2017.

[6] S.Uma, R.Maheshwari, J. K.Mayuri, R.Sowndharya, S.VanoJenifa, "Design of a Secure Block Chain based E-Voting System,"*International Journal of Research in Engineering, Science and Management* ,vol 2, issue 3, March, 2019.

[7] Parimi Shiva Kalyan, V. Kakulapati,Parimi Arvind, "Blockchain based Application to Curb Hoaxes on Social Media using Decentralized Voting System,"*International Journal of Engineering and Advanced Technology (IJEAT),*,ISSN: 2249 8958,Volume 8, Issue 4, April 2019.

[8] Yang JunHo, Jin MinGoo Lee, KyungHee, Cho Jungwo, " Campus e-Voting System on campus based on Block Chain Security Technology,"*in the Proceedings of The KACE,*pp. 67-70, Aug. 2018.

[9] Nir Kshetri, Jeffrey Voas, "Blockchain-Enabled E-Voting",*IEEE Software*,vol 35, issue: 4 ,July 2018 .

[10] Ashish Singh, Kakali Chatterjee , "SecEVS : Secure Electronic Voting System Using Blockchain Technology," *2018 International Conference on Computing, Power and Communication Technologies (GUCON),*Greater Noida, India,28-29 Sept. 2018.

[11] Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol 7, pp. 24477 - 24488, Feb 2019.

[12] Hsin-Te Wu, Chang-Yi Yang, "A Blockchain-Based Network Security Mechanism for Voting Systems",*2018 1st International Cognitive Cities Conference (IC3)*, Okinawa, Japan, 7-9 Aug. 2018.