IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

Blockchain in Voting

Adwait Dabholkar[1], Dr.Pravin Gundalwar[2]

M.C.A Student, MET Institute of Computer Science, University of Mumbai, India[1]

Associate Professor, MET Institute of Computer Science, University of Mumbai, India[2]

Abstract:Even Though the technology Blockchain was invented in 1991 by Dr W.Scott Stornetta, it is well Known to be used in cryptocurrencies for example bitcoin one of the most famous cryptocurrency introduced by Satoshi Nakamoto in 2008.Blockchain also Offers new opportunities to develop many types of applications and digital services. In this Paper we are going to discuss the use of the open source blockchain technology in electronic voting system that can be used in local or national elections that can deliver fraud-less, reliable & Secure voting system.

Keywords: Blockchain ,Voting, Decentralized Voting, e- voting

I. INTRODUCTION

There are two types of voting system widely used around the world

- EVM (Electronic Voting Machines)
- Ballot Papers

A. EVM:

EVM(Electronic Voting Machine) was used used in National elections of Estonia followed by Norway. Aim of EVM is to provide sec,anonymity from outside interference and maintain the privacy of voter.EVM Consist of control units and balloting unit connected to each other by five meter cable to electronic ballot box with its interface having a button for each choice.

The EVM is accessible by only one ballot number ensuring that only one person gets to vote once only.

Problems with EVM

Software Security

- Software used in EVM is only considered secured if Source Code is Genuine.
- The Contents stored in micro-controllers in EVMS cannot be read back or reverified rendering it untrustworthy.

Hardware

- EVM Manufacturers use generic Micro-controller even though it much less secured from FGPA Microcontroller or AISC Microcontroller.
- The components of the EVM system,the Micro-controller,Motherboard can be easily replaced Hacking
- There are incidents and reports of EVMS being Hacked prior elections and after the elections.
- The EVM System uses dual EEPROM to store data or votes.
- EEPROMS are highly unsecured and stored data can be manipulated from external source.

EVM cannot verify the votes of the voter in case if voter wants to find if his votes are alloted to his/her desired political party and is rejected by countries like Ireland,Italy and Germany.[3]

B. Ballot Paper

A ballot device used to cast votes in an election, and may be a piece of paper or a small ball used in secret voting. It was originally a small ball used to record decisions made by voters.

Each voter uses one ballot, and ballots are not shared. In the simplest elections, a ballot may be a simple scrap of paper on which each voter writes in the name of a candidate, but governmental elections use preprinted ballots to protect the secrecy of votes. The voter casts their ballot in a box at a polling stations.

Problems with Ballot Paper Voting

Ballot vote process is very tedious and cumbersome process and lots of Man power is required to perform the entire process.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

Booth Capturing
The Fraudulent party can beat or bribe the voting officials and fill the box with ballot papers. It will be difficult to separate the legitimate votes from the fake ones even if the officials file the complaint against fraudulent party.

Ballot paper stealing
The Votes can be stolen from the ballot during logistic and transportation of ballot papers to center where the votes are counted after the elections are done.

Invalid Votes
A simple ballot paper system is where a paper is like a chess board with squares drawn it it with contestant name and party symbol. In order to cast he vote the voter is handed a stamp ,which he has to use to stamp on his/her desired party or candidate. It is absolutely mandatory that the stamp mark should be exactly in the square the voter want to wants to vote or else the voted is counted as invalid.

Counting:
Counting is the major setback of Ballot Paper Voting. If used in nations like USA,India,China
Counting each and every vote of every citizen can be hectic and tiresome and requires huge manpower.[4]

II. THE BLOCKCHAIN SOLUTION

Blockchain is a shared ledger where data stored is secured by hashes and is replicated amongst its peers or the entity in the network.

As shown in Fig 1 below the Data stored in Blockchain is in the form of blocks of transaction with each block having its own hash which is calculated by passing the data,nonce,timestamp and previous hash through SHA256 hashing function which returns a 256 bit hash,this hash is further included in the Second block and the hash of the Second block is calculated and passed on to the Third block hence forming a chain of transactions.
As More and More Transactions are added into the Blockchain more difficult it gets to tamper the data,because tampering with one Block will break the link of all its blocks after it.

As shown below in Fig 1 the block 0 is the Genesis block that is the first block which is created when the ledger is initialized which has nonce,data,previous hash and current hash set to null.

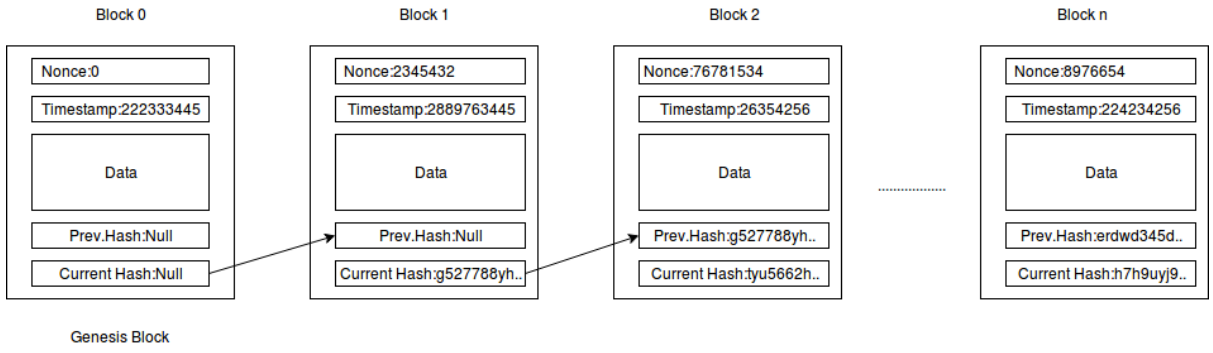

Fig. 1 Transaction Blocks in Blockchain

Every Peer in the Blockchain Network is assigned a certificate which is used to sign the transactions which get commited on the ledger.
As Shown in Fig 2 below shows the connection and transactional flow betwwen peers. Once a transaction is committed on a single peer on the network provided it is valid that transaction is forwarded and committed on all other entities or peer connected to each other in the Blockchain network. The Peer or Entities in the network are connected to each other in peer-to-peer fashion hence it is also called as Serverless or decentralized architecture.[1][5][6]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

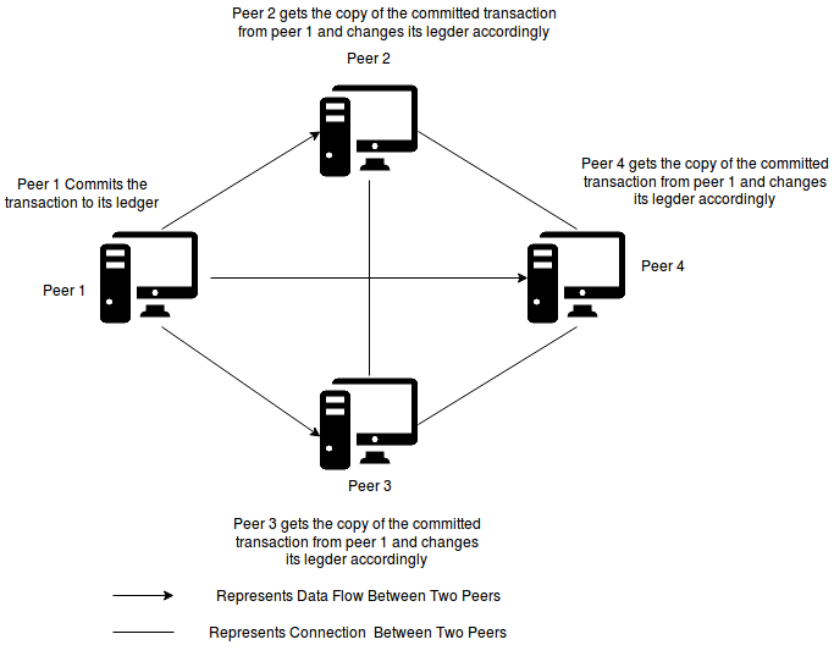

Fig. 2 Connection and Transactional Flow of Blockchain Network

Before the blocks are commited on the ledger the state of the ledger at all the peers is matched. If a Peer transaction blocks are tampered,it will go out of sync with other peers resulting other peers not accepting transaction from the fraudulent peer.[1][5][6]

III.BLOCKCHAIN SOLUTION IN VOTING

Lets Consider a Scenario where there are three political parties participating in an election.

- Party A
- Party B
- Party C

Each political party is given two machines or voting machines .

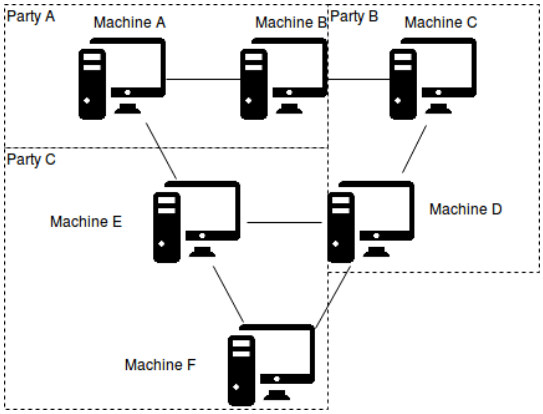

Fig.3 Peers in Control of their respective Politica Party

As shown in Fig 3 above party A is in-charge of machine A & B, party B is in in-charge of Machine C,D and Party C is incharge of Machine E and F.
The Machine A,B,C,D,E,F are connected to each other in peer to peer connection forming a blockchain network which is shown in Figure 4 below.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

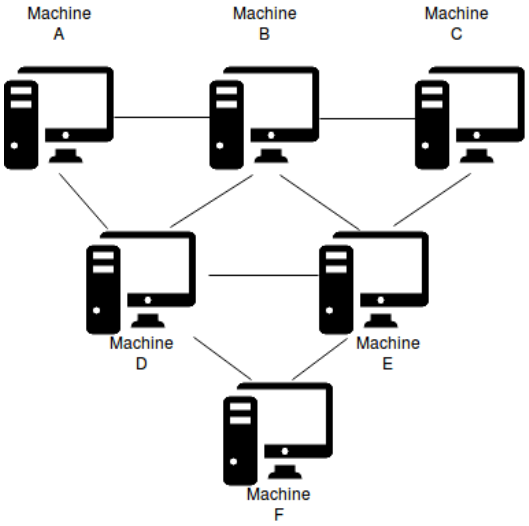

Fig.4 Voting Peers connected in Peer to Peer fashion

Suppose a voter who wants to cast his vote uses for example Machine E. Then Vote will be registered in the following sequence

- The Voter Validates his identity and his right to vote by inputing his voter id.
- Voter choses the party to which he wants to cast his vote to.
- Vote gets registered as a transaction which is signed by the identity certificate of Machine E(As the voter voted from Machine E along with the time stamp)
- This Signed transaction is distributed amongst all the peers that is machines A,B,C,D,F which are connected to each other in blockchain network.

Attempt to Fraud
Machines A,B,C,D,E,D,F are Connected to Each Other in peer to peer Blockchain network.
If a fraudster tries to fiddle or mess with the transactions in any Machine, suppose Machine A then
1. Then he has to change all the transactions block in the ledger as each block is protected with its own hash and previous block's hash included in it.
This a nearly impossible task as the fraudster has to manipulate each and every block in the ledger.
2. Lets say that the fraudster manages to manipulate each and every block in the ledger but to prove authenticity he has to replicate the ledger's faulty transactions on all the machines connected in the network which is impossible task if the blockchain network is huge containing more than 500+ peers with each political party having its control on a given set of peers/machines.[1][5]

IV. CONCLUSION

We have proposed a decentralized tamper-proof Blockchain voting system assuming that the voter casts his/her vote on a secured device/machine. Any registered Voter can vote through any device connected to the voting Blockchain Network. The Blockchain is publicly verifiable and due its distributed and decentralized property no Fraudster /hacker will be able to manipulate or corrupt it.

REFERENCES

[1]. ALEX TAPSCOTT AND DON TAPSCOTT , BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD ,ISBN:1101980133 9781101980132
[2]. Andreas M. Antonopoulos.,Mastering Bitcoin: Programming the Open Blockchain,O'Reilly Media
[3]. http://kanglaonline.com/2012/03/how-can-electronic-voting-machines-evm-be-manipulated/
[4]. https://www.quora.com/Why-does-India-not-use-ballot-papers-for-voting
[5]. https://www.thebalance.com/how-the-blockchain-will-change-how-we-vote-4012008
[6]. Ahmed Ben Ayed, A Conceptual Secured Blockchain based Electronic Voting System, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017