

Report On: Blockchain in e-voting

Submitted to:

**Dr. S Venkatesan**

**4304, CC-II**

**Indian Institute of Information Technology - Allahabad**

**Devghat, Jhalwa,**

**Allahabad 211 015, (UP) INDIA**

**Submitted by:**

**ADITYA VERMA, MIT2018064**

**HIMANSHU CHAUDHARY, MIT2018037**

**TAPASWINEE SETHY, MIT2018073**

**IIIT ALLAHABAD**

FLAWS IN CONVENTIONAL VOTING SYSTEM

* Security and Transparency is a threat.
* Use of centralised system - Full control to one organisation - Both on database and system.
* It’s possible to tamper database present at one place.

How Blockchain concept can help?

* Blockchain is distributed digitally to a number of computers in almost real time.
* Blockchain is decentralized, the entire recording is available for all users and peer to peer network users. This eliminates the need for central authorities, such as banks, as well as trusted intermediaries.
* Blockchain uses many participants in the network to reach consensus.
* Blockchain uses cryptography and digital signatures to prove identity.
* Blockchain has a difficult (but possibly) mechanism for altering stored records.
* A Blockchain is time-stamped. - Transactions in blockchain are timed, so they are useful for tracking and verifying information
* High Availability: Distributed completely to all nodes and stored in the database completely.
* Verifiability and Integrity: Each block is verified and added to the blockchain. Therefore, it will be difficult to change the data in it because all the blocks have to be changed value.

HOW CAN WE USE BLOCKCHAIN?

* We can record voting results from every election booth time to time during the election process.
* Most people today don’t trust their governments for fair electoral practices

Problems in conventional voting system?

* Takes 3-7 days for result estimation, after the voting process gets over.
* Data manipulation, security and transparency.

“Make DATABASE PUBLIC! Distributed over several nodes.”

BLOCK STRUCTURE

* Node id
* Timestamp
* Voting result - kind of histogram
* Hash of previous node
* Digital signature of node

Before Voting Process…..

* Every Voting Booth needs to register itself as a node in the network before the voting process starts.
* This is kind of a Permissioned Blockchain used here, where each node in the network has previously acquired some sort of permission to be in the network. There is no option of nodes to get dynamically added into the network.

During Voting Process …..

* Time to time, we are going to update our blockchain by adding further blocks of transactions into it.
* Each transaction, represents a vote here.
* Each booth represents a node in the permissioned blockchain network.
* During the voting process, suppose we maintain upon adding the transactions onto the blockchain after 10 mins, then after every 10 mins we will be adding new blocks to the blockchain.
* We can check the digital signature of the node, from which the block is coming in order to check if that’s the same node through which we intend to get the block or not.

After voting process…..

* After voting process gets over, we can just traverse the whole blockchain to see the election results as well as to see whether the blockchain’s integrity is intact or not.
* We can match previously acquired Hash values with the Hash values present in the Blockchain in order to test Integrity of the system.

How security is offered in our approach?

* Hash - The hash of previous block is stored in the present block, forming a hash chain, in which if something gets modified the whole hash values present in the blockchain will get modified. SHA-256 is used for this purpose.
* Digital signature - This is used to verify the identity of the block coming from some node or not. ECDSA is used for this. ECDSA is better than DSA, level of security is same but with a smaller key length, allowing for faster calculations.
* Continuously adding of block - continous adding of block into the blockchain helps the chain to grow at faster rate.
* Authorisation - voting booths get initially added as node in the network. Whole network is a permissioned one.
* PBFT algorithms (Practical byzantine fault tolerance) - is used for consensus purposes.

Another approach

* Every voter and candidates can be registered in the Permissioned Blockchain Network as network entities.
* Initially, each voter will be granted one coin which they can cast to some candidate.
* Cast of vote/ transfering of the coin to the candidate’s account just needs bitcoin architecture underneath.
* After whole process gets done, we can count the number of coins received by the candidates to decide the winner.