‘*Blockchaining’ Democracy*

Suprit Atul Gandhi[1], Milind Nilesh Gawde[2], Hasan Mohammad Shahid[3]
Department of Computer and IT
College of Engineering, Pune
[1]*supritgandhi@gmail.com,* [2]*milindnileshgawde@gmail.com,* [3]*hasan.mshahid2522@gmail.com*

***Abstract*—The very survival of democracy lies in election. Yet, in the 21st century where electronic electoral ballots are used there exists a slightest chance of voting machine tampering. Frequent allegations by some politicians regarding tampering and the rise of blockchaining ecosystem gave a firm support to this idea. Using this idea, elections not only will be more secured for a highly populated democracy like India but also, it will foster a larger participation of public, since they can vote from home too.**

Keywords—Blockchain, Genesis block, Chain integrity, Hashing.

I. INTRODUCTION

Democracy and elections were gift to mankind from the Greeks. But to make this system more transparent, ballot system emerged. Since, ballot systems either physical or electronic aren’t safe due to either lack of use of cryptography or its simple implementation.

The idea of blockchain emerged from the existing theory of **Merkle trees** which basically involve a datablock as a leaf node and hashed values as parent nodes. So, the datablocks are secured to a particular extent due to hashing of previous hashes. The combination of attachment of timestamp to this very tree or chain emerges into vague idea of blockchain. Blockchains are currently used for virtual currency transactions due to the high security it provides during this process.

Blockchains became more popular thanks to ever increasing trading in **‘Bitcoins, Ethereum platform, Litecoins, etc’.** Thus the security of blockchain can be extended to encourage the world suffrage by designing a voting system on this very basis.

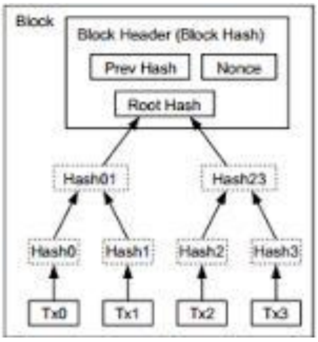

Fig.1: Merkle tree

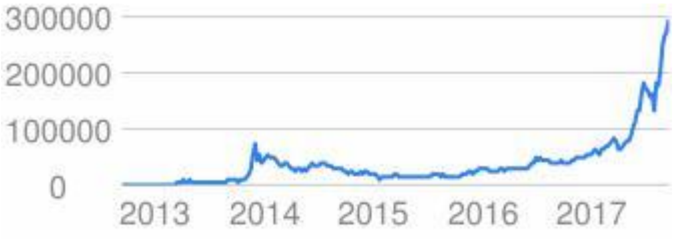

Fig.2: Year vs. value of bitcoin graph

II. EXISTING SOLUTION

Nearly all democratic countries rely on electronic ballot system, this system has a low latency time due to the data directly registered at the hardware level, but it has a bad trade off with the security of the system as the local database can be mishandled easily creating confusion in the public. To counter this problem we can trade off with a bit higher latency with much improved security by implementing a blockchain system of votes.

III. Overview Of The Solution

The solution involves creating blockchains using hashing of timestamp, a previous hash and a particular ID allotted by the country example: Social Security Number, UIDAI for India, etc can be effectively used.

IV. Algorithm

The chain will initiate with the **genesis block[first block]** which will be hardcoded by the **Highest Authority** and **Election Commission** of the State. The essence of blockchain lies with the hashing of data of the previous block in order to maintain the integrity of the data. Available, cryptographic algorithms such as **SHA-256**, **SHA-512, scrypt, bcrypt, PBKDF2; salting can also be used here.** In case of salting, the salting bit/s will depend on the unique identification number provided by the government. This hashing is in no way related to 'mining', since there is no **PROOF OF WORK** problem to solve.

After the genesis block, data of each block that is the identification number will be entered by the user whereas index, hash and timestamp will be auto-updated by the system chain.
Validation of integrity of blocks is an essential factor to accept that block in that chain, each chain corresponds to the 'Party' you are voting which means the winner is the one with the longest chain. Also, an essential part involves sharing and syncing one node with other nodes of blockchain when a node generates a new block it should broadcast to the network. When a node connects to a new peer it queries for the latest block. When a node encounters that has an index a block that has an index larger than the current known block, it either adds the block to the current chain or queries for full blockchain.

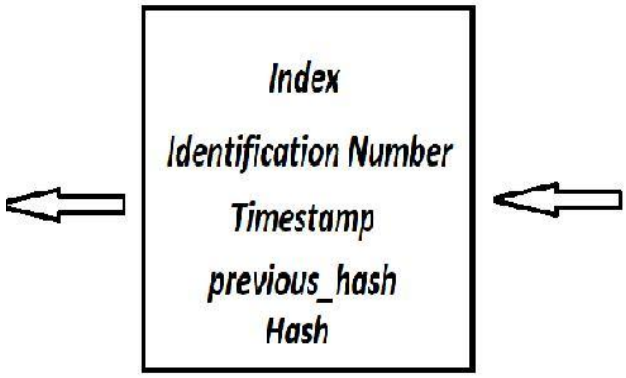

Fig.3: Arrows indicate the Flow of hash

$$hash\_value = Hash(index + identification\ number + timestamp + previous\_hash + salt)$$

salt - is stored in main government server corresponding to each identification number.
index - serial number of block in a chain
identification number - which is issued by government
Example : UIDAI for India.
timestamp - time at which the vote was recorded
previous_hash - communicated hash of previous node

Fig.4: Hashing Equation

V. Pseudocode

Block Structure:

```
class block_definition() {
        index;
        identification number;
        timestamp;
        hash;
        previous_hash;
}
```

Hashing of block:

```
function hashing(block){
        return
        SHA256_hashing_of_timestamp+identification number+index+previous hash+salt
}
```

Salt will be available in the government server archive unique to each identification number.

Genesis Block:

```
    function genesis_creator(){
            return new block(block_info of the President
            of the State with digital signature);
    }
```

Validation of integrity:

```
    function validation(newBlock, oldBlock){
        if(next_index != index+1)
                return false;

        if(previousBlock.hash!=newBlock.previous_hash)
                return false;

        return true;
    }
```

Length of chain:

```
    function valid_or_not(new){
      if(Valid(new) and new.length > blockchain.length)
                return true;
     return false;
  }
```

VI. Conclusion

Maintenance of integrity combined with encrypted blockchains provide a much clear solution to the very existence of democracy. This will foster people to exercise their right to vote, since elections booths are nothing but our personal computers.

REFERENCES

[1] https://www.blockchain.com/
[2] https://en.wikipedia.org/wiki/Merkle_tree
[3] http://fortune.com/2017/05/23/blockchain-chasm- of-death-bitcoin/
[4] https://www.raconteur.net/business/the-future- of-blockchain-in-8-charts
[5] https://en.wikipedia.org/wiki/Blockchain
[6] Ethereum White Paper