Any Time Voting System using Blockchain

Nandakishore VV[1] and Amal C Saji[2]

Abstract— **Any Time Voting system(ATV) employs blockchain technology to allow voters to cast their valuable votes securely, in a hassle free fashion, with assurance that electoral fraud is impossible. Voting shall remain open for multiple days, ie; it is not limited to a single day.**

I. INTRODUCTION

Election is a huge administrative process that takes up a lot of time, effort and monetary resources of a state. In a country like India, where assembly elections are not held uniformly, the entire voting process demands large scale financial needs, workforce and infrastructure. Despite all the shortcomings it has, a lot of countries still follow the traditional paper ballot system. India has adopted Electronic Voting Machines(EVMs) from 1999 and by 2017, EVMs have replaced paper ballots all over the country. Even though EVMs are one of the most secure voting systems, they are not yet fully foolproof.

II. PRESENT DAY SCENARIO

The present day voting systems, be it paper ballots or EVMs, require armed forces guarding them to ensure the security of the votes cast. Election period witnesses booth capturing to confiscate ballots/EVMs, identity fraud and violence in many parts of the country. Election process demands a large number of government officials to work overtime for the overall management and the necessary paperwork. This indicates that elections aren't carried out efficiently and that their security and transparency should be improved.

III. WHY BLOCKCHAIN?

Blockchain is a decentralized distributed public ledgering system. It can be used for secure monetary transactions, data storage and retrieval. The problems of the now prevalent EVMs can be overcome if we implement voting using blockchain technology. It is the most secure technology available now which promises the prevention of identity fraud and multiple voting. This problem can be solved successfully only by using blockchain as all the other implementation techniques use a traditional database which could be compromised.

Blockchain is a disruptive technology and if e-voting is enabled using blockchain, it would disrupt the traditional election process and the working of the election commission in the country. The entire process would become simple and less complicated. The data saved in the blockchain is immutable, unlike the data in conventional servers. Moreover, the overall expense of the entire election process across the country could be reduced. Public holidays need not be declared in regard with elections, if this system is implemented. Votes once cast are not destroyed or mutable, even if the voting systems are damaged. Therefore, the number of security personnels at the voting centers can be reduced considerably. If a voting system is damaged, voters can make use of other voting systems in the same locality with no issues whatsoever. The counting process and result declaration is made hassle free and simple because votes are counted as they are being cast. The system also follows green protocol and is environment friendly.

IV. IMPLEMENTATION

A. Voter Database

The electoral roll database can be maintained in a blockchain. Biometric information of the voters are collected and hashed using SHA256 algorithm. A specific key is generated for each citizen from the hash. This cryptographically secure key is now stored in a blockchain. From this database, the citizens who meet the criteria for casting a vote are assigned with token values set as true and are given a private key by the election commissioner before each election is declared. The admin(election commissioner)adds the candidates after the nomination scrutiny and they are given a token, a private key and wallet value initially set as zero.

B. Any Time Voting

The Election Commissioner decides a period of time when votes can be cast, ie; election process is not confined to a single day. Votes can be cast by eligible voters at any time, using ATVs. Any Time Voting system is a specially designed online platform which would be installed in multiple places in all constituencies. ATVs are equipped with biometric sensors which would be used to confirm the voter's identity. The biometric information is collected from the ATV and hashed using SHA256. Voter enters a key which is hashed and checked against the hashed keys saved in the voter database. If a match is found, the corresponding hashed value of the biometric information is fetched from the database. This biometric hash is compared with the currently hashed biometric value to identify voters. If the key is matched, the voting screen is enabled and votes can be cast.

[1] Nandakishore VV, S5 Master of Computer Applications, College of Engineering, Trivandrum

[2] Amal C Saji, S5 Master of Computer Applications, College of Engineering, Trivandrum

C. Voting process

Voting can be done only if the voter has their token value set as 'true'. A voter clicks on the name of the candidate and then the token of the voter is set as false. Simultaneously, the wallet value of the candidate is increased. The vote is displayed on screen for confirmation.

D. Result Declaration

Once the election period has ended, the admin(CEC) can allow the privilege for all the voters to view the number of votes secured by each candidate.

V. Technical Implementation

Smart Contract: It is a computer program that controls the voting process. Each vote is considered as a transaction and is recorded into the blockchain based on this Smart Contract. The contract is written using Solidity and compiled using pragma solidity $\hat{0}$.4.0
Ethereum Blockchain: Voting is a token based transaction to implement the system Ethereum which was developed by Vitalik Buterin, is used.
NodeJS: The front end of the application is developed using NodeJS since it is fast and dynamic.
Ganche-cli: The personal blockchain for Ethereum development

Let Upr be the private key of the user, Ubio be the biometric information collected from the user. H is a hashing function that hashes the Ubio.

Algorithm 1 AUTHENTICATE()

```
Let Upr ← User private key, Ubio ← User Biometric
    information
DbHash ← DBACCESS(Upr)
Hbio ← H(Ubio)
if Hbio = DbHash then
    return true
else
    return false
End procedure
```

Hkey is the hashed value of the users private key. Vdb is the voter database that stores the hashed biometric information and users private key as key value pairs. DkHash stores the hashed biometric information of users.

Algorithm 2 DBACCESS(Upr)

```
DbHash ← 0
Hkey ← H(Upr)
if Hkey in Vdb(DkHash) then
    return DbHash of Vdb(DkHash)
else
    DbHash ←0
End procedure
```

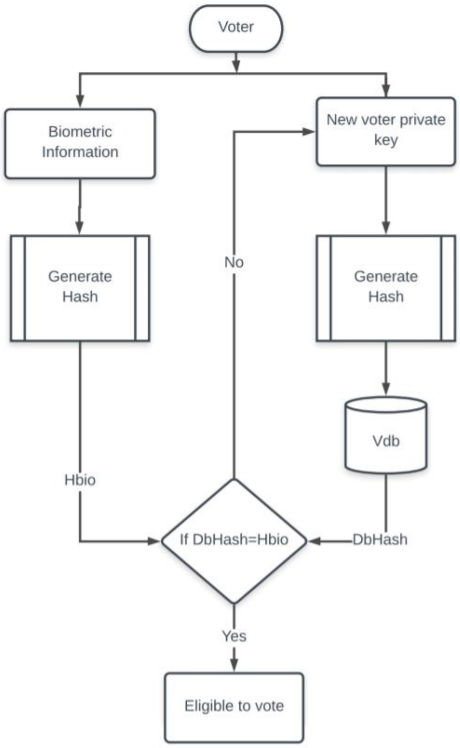

Fig. 1. Voter Identification

VI. Future Scope, Challenges

The future scope of blockchain enabled E-voting is extensive. Instead of using public ATVs, voting could be carried out using mobile phones having an internet connection. An Adhaar model blockchain database could be created with all the personal details of a citizen, thereby making financial transactions easy and traceable. It will also make the scrutiny of candidate nomination simple. Administrative level implementation of the blockchain would make the functioning of the governments more transparent than ever before.
Any Time Voting has the potential to disrupt the whole election process and it would be challenging to implement as it could be difficult to win the confidence of the authorities and general public. Even though it raises concern for a section of people, yet it holds the promise of making elections more transparent, secure and would encourage people to exercise their voting right.

References

[1] 1. Sachidanand Sing and Nirmala Singh, Blockchain: Future of Financial and Cyber Security,2016 2nd International Conference on Contemporary Computing and Informatics (ic3i), 978-1-5090-5256-1/16/ c 2016 IEEE.

[2] 2. Nir Kshetri and Jeffrey Voas, Blockchain-Enabled E-Voting. IEEE SOFTWARE, 0740-7459/18/ 2018 IEEE.

[3] Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland, Decentralizing privacy: using blockchain to protect personal data. IEEE 2015.