Review on E voting System using Decentralized, Immutable and Transparent Blockchain Technology with Privacy Protocols

Mr. Nikhil Patare [(1)], Mr. Shubham Adsul [(2)], Ms.Dhanashri Durge [(3)],

Prof. Monali Mohite [(4)]

[(1)]Student, Dept. of Computer Engineering, BSIOTR, Wagholi, SPPU, India
[(2)]Student, Dept. of Computer Engineering, BSIOTR, Wagholi SPPU, India
[(3)]Student, Dept. of Computer Engineering, BSIOTR, Wagholi, SPPU, India
[(4)]Professor, Dept. of Computer Engineering, BSIOTR, Wagholi, SPPU, India

[(1)]E-Mail: nikspatare1998@gmail.com, [(2)]E-Mail: shubhamadsul2222@gmail.com, [(3)]

E-Mail: dhanashri.durge1997@gmail.com, [(4)]E-Mail: monalipmohite@gmail.com

Abstract

This system is an attempt to suggest blockchain technology for digital voting system. Elections and voting are important factors of a democratic country, however the voting process is increasingly challenged by the power of the internet. There are security problems around electronic voting booths, which analyzers have warned are vulnerable and easy for hacking. Such weak system could be used to undermine trust in an election system. The blockchain technology is presented as a game changer for many of the existing and emerging technologies. With its immutability and transparent property and decentralized and unique architecture, it is taking important platform in many services as an equalization factor to the current parity between consumers and large corporate companies. This paper presents an effort to advantage of blockchain such as cryptographic foundations and transparent system to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verification.

Keywords: Blockchain, Voting booths, Vulnerable, Decentralized, Immutable

1. Introduction

Democratic voting is a crital and serious event in any democratic country. The most simple and common way in which a country do voting through a paper based system but it has many drawback like time complex process , security of voter etc which makes the lead of digital voting. Digital voting is the use of electronic devices, such as voting machines, EVM's. Nowadays e- Voting is a unique solution that simply and conveniently helps to capture people in the governance process. One way to get solution these security documents problems through the blockchain technology. In simple terms, blockchain is a link between the different blocks. Blockchain technology is hold up by distributed network. It composed of a large number of interlinked nodes and each node having the past of transaction. If major part of nodes having same opinion and agree then only transaction is accepted. Basically blockchain technology gives a successful way to make e-voting more acceptable and efficient way. Advantages of e-voting using blockchains includes: i) greater transparency due to open and distributed ledgers, ii) inherent anonymity, iii) security and reliability iv) immutability.

2. Related Work

2.1 Blockchain Working

Blockchain was first launch by Satoshi Nakamoto [1], who proposed a peer to-peer payment system that allows cash transactions through the web without depend on trustor the stand in need for a financial institution [2]. Blockchain is secure by plan, and an example of a system with a high intricate failure tolerance [3]. Blockchain is the digital, distributed, and decentralized ledger latent of most virtual currencies that's control for logging all transactions unsorted by the need for a financial intermediary, such as a bank. In other words, it's a new means of pass on funds and logging details. The first block in a blockchain is known as the ‘Genesis block’ or ‘Block 0’. The genesis block is normally hardcoded into the software; it is special in that it doesn’t contain an allusion of a previous block[4]. Once the genesis block has been started ‘Block 1’ is created and when complete is linked to the genesis block

Field	**Description**	**Size**
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypt d almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transaction size.

Table 1. Blockchain Structure

A blockchain is designed to be accessed across a peer-to-peer network, every node then in contact with other nodes for block and transaction interchange. Once connected to the network, peers start dispatch messages about other peers on the network; this creates a decentralized method of peer discovery. The grounds of the nodes within the network is to validate unsettled transactions and recently mined blocks, before a new node can start to do this it first has to convey of an initial block download.

2.2 Existing Voting System

Electronic Voting Machines are being used in Indian General and state election to instrument electronic voting in bit from 1999 elections and in the last in 2017 state elections hold on in five states over India. EVMs have substitute paper ballots in local, state and general elections in India. There were earlier asserting regarding EVMs' temper and fraud capability and security which have not been proved yet. Drawback of EVM or Existing Voting System. 1) Vulnerability, 2) Susceptibility to fraud, 3) Malicious programming.

2.3 Proposed Voting System

2.3.1 Registration of Voter

The first feature of our design is the registration process, verifying a voter is crucial in set up security within the system. Making sure that someone’s identity isn’t being misused for cheating purposes is main factor, mostly when voting is considered, where every vote have value.

1. Initially, a transaction is created when a voter ‘registers’.
2. The next transaction is generated when a government miner permit that user’s right to vote

2.3.2 System Architecture

When determining on the architecture we took powerful inspiration from both the distributed and acquirability of the Bitcoin network and the gathering process of traditional voting. The network is a multi-tiered, decentralized infrastructure which having the two definite blockchains. A local node is setup to only be in contact with the other local nodes under the connected constituency node and the constituency node itself.

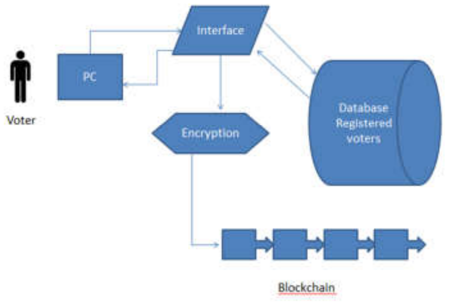

Fig 1.Architecture of E-voting System

2.3.1 Voting Process

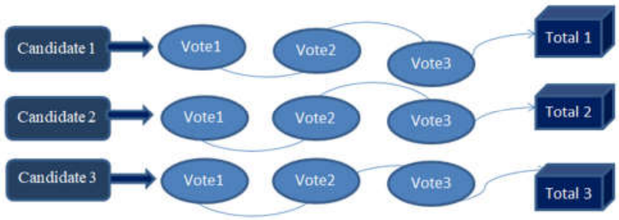

Fig 2.Additing vote into blockchain of E-voting System

(1)Requesting user to vote: The user will have to log in to the voting system using his credentials- in this case, the e-Voting system will use his Social Security Number his address, and the voting confirmation numbers suggested to registered voters by the local authorities.

(2) Casting a vote: Voters will have to select to either vote for one of the candidates or cast a protest vote. Casting the vote will be proceeds through a user friendly interface

.

(3) Encrypting votes: After successful execution of casting vote, the system will create an input that consist of the voter identification number came after the complete name of the voter and the hash code of the earlier vote. This way each input will be unique and make sure that the encrypted output will be unique as well.

.

(4) Adding the vote to the Blockchain: Choose the information is recorded in the particular Blockchain. Each block gets attached to the previously cast vote.

3. Conclusion

To close, our service proposal consist of of a geographically distributed network made up of machines from both government and public substructure; this substructure houses two separate blockchains, one for voter information such as who has voted and the other for vote information such as what has been voted. These blockchains are held completely separately to remove any threat to link votes for certain parties back to perticular voters while maintaining the ability to track who has voted and how many votes are actually available. Due to the encryption mechanism we are using it would be close to beyond the bounds of possibility for any person to gain access to all the votes.

Acknowledgments

The authors wish to thank Prof. Monali Mohite Project Guide, Prof. G.M. Bhandari Head of Computer Department for supporting this research study through survey sessions.

References

[1] National Institute of Standards and Technology, "Federal Information Processing Standards Publication", (2012).

[2] S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).

[3] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. (2013), pp. 1-27.

[4]Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block (Accessed 27 September 2016)

[5] J. R. Douceur, "The Sybil Attack", International Workshop on Peer-to-Peer Systems, (2002), pp. 251-260.

[6]bitcoin/src/chainparams.cpp,https://github.com/bitcoin/bitcoin/blob/3955c3940eff83518c186facfec 6f 50545b5aab5/src/chainparams.cpp#L123

[7]Bitcoin Block Explorer, https://blockexplorer.com

[8] Why Use Bitcoin? http://www.coindesk.com/information/why-usebitcoin/

[9] How to Set Up a Bitcoin Miner, http://www.coindesk.com/information/how-to-set-up-a-miner

[10] Elliptic-curve digital signatures, http://davidederosa.com/basicblockchain-programming/elliptic-curve-digital-signatures/