JOURNAL OF MECHANICS OF CONTINUA AND
MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-16, No.-10, October (2021) pp 1-8 ISSN (Print) 0973-8975

A FRAMEWORK BASED ON BLOCKCHAIN FOR ELECTORAL VOTING SYSTEM

Tarun Kumar

CSED, SET, Central University of Rajasthan, Ajmer (India)

Email: tarun.kumar@curaj.ac.in

https://doi.org/10.26782/jmcms.2021.10.00001

(Received: July 27, 2021; Accepted: September 20, 2021)

Abstract

Electoral voting system is the pillar to maintain the democratic freedom of any country. The fair and transparent organization of election is the basic need of the country. Many countries are basically using one of two ways to conduct election either using ballot paper or using electronic voting machines. Each one has its own pros and cons. The fast, trust and e-voting is the need of the future. In recent years, blockchain technology is rapidly adopted in various fields by various organizations. The Decentralized and cryptographic algorithms are the major reason behind this. Considering the increasing issue of security, trust in the traditional Voting System and future requirements, this paper proposes a framework for an E-Voting system based on blockchain technology. This paper discusses the network architecture for blockchain technology, framing the processing casting votes and counting of votes. The analysis of various issues and challenges in the electoral system is carried out in the context of the proposed framework. This framework may improve the security and decreases the cost of hosting nationwide elections.

Keywords: Blockchain Technology, E-Voting, SHA256, P2P Networks, E-Voting

I. Introduction

Blockchain technology is growing and being in demand in present. The immutability and maintaining secure records attracting many industries to adopt this technology. The Blockchain technology defines a underlying concepts of recording transaction in cryptographically secure and linked manner. The various crypto-currencies, insurance organizations, financial organizations, supply chain management companies etc. are started using blockchain technology. Like other technological tools, Blockchain also provides business benefit. Although there is a high level of information content about blockchain technology have successful implementations not caught up with the volume of publications. Blockchain is an emerging technology in the computer science field with different applications. It is an open, general ledger that records transactions between two parties efficiently, securely and verifiably. It's an ever-growing list of records called blocks, which are linked and backed up using cryptography. For using blockchain as a distributed ledger, it is generally implemented by a peer-to-peer network in which each peer adheres a protocol for communication between nodes and validation of blocks. Once added, the information in any particular block cannot be changed without medication of all subsequent blocks in blockchain, which requires permission of majority of the network. Although blockchain records are alterable, blockchain is considerably secure by design and it work as a distributed computing system with high fault tolerance.

Apart from this, the electoral voting system in many countries likes India is using Electronic voting machines to conduct elections. These machines based voting system is not only outdated but it has various limitation of offline voting. Nowadays, increasing trust issues on EVMs by various organizations is also problematic. The election process must be transparent and unbiased. Due to the huge population, traditional voting system fails as many people are not verified properly before the process of voting and hence resulting in problems like fake voting or double voting. Also, there are many other flaws that occur and sometimes the transparency is not maintained. To overcome these limitations, this paper proposes a novel voting system that is based on blockchain technology. This paper discusses all the aspects if this system i.e network architecture, voting process and vote counting process. The aims of this system are to provide transparent, secure and trustable voting system for general electoral process. This system also provide flexibilities to voters for casting votes from any of the official booth instead of the dedicated to booth. Next sections discuss the existing works and proposed approach in detail.

II. Literature Review

Initially blockchain concept is formulized by Nakamoto [IX] by proposing world's first Cryptocurrency called Bitcoin. This Cryptocurrency is based on cryptographically secure chain of blocks distributed over the peer-peer nodes. The blocks are linked with each other using the hash of the block. This hash is computed using secure hash algorithm (SHA256) [I]. This has algorithm generates one way hash i.e. it is not possible to generate value using hash. This property of the SHA256 algorithms adds immutability in the blockchain. The decentralization and trusted consensus algorithm remove the need of third-party authority to verify the transactions. The Bitcoin provides incentives to the peer-peer nodes to validate and maintain the transactions. This concept also provides a mathematical proof that this Cryptocurrency can never be hijack. To hijack the network, the hijacking of majority of the nodes is required which is practically not possible. The blockchain technology gained popularity from various organizations, industries and researchers. These start looking the application of blockchain technology in their respective applications [XI]. One of the use case of blockchain technology is proposed by Hobert and Litchfiled [IV] in software industry. In this use case, the software license policy is implemented on the blockchain technology. This preserve the privacy and various version based policies. Another use case for software industry is proposed by Litchfiled and Hobert [VII] to validate the software licensing across the different platform. As the security and transaction validation in blockchain is performed by various consensus algorithms i.e Proof-of-work (PoW), Proof-of-Stake, Proof-of-trust, proof-of-existence etc. [XI],[V],[II]. The similar application scope of the blockchain technology is proposed by Lemieux [VI] to maintain integrity of digital documents. This domain of this application is not financial. Hence, it opens up the wide area of scope where blockchain technology can be applied. Ferrer et al. [II] proposed an application of blockchain to records the hash of online files preserve their existence using PoE algorithms. Any user can verify the existence of file in the network. This is helpful to maintain the copyrights of the digital documents, assets, software, videos etc. This application can be utilized in generating ownership of the digital data and documents [III]. Mallick and Kushwaha [VIII] use blockchain based applications for implementing publish-subscribe system. User can subscribe any available topics, and subscribe can post the notifications to the respective subscriber. The p2p network is the foundation of the blockchain technology and this involves transferring the large amount of the data across the nodes. This generates the packet flooding in the network. Hence, some researchers are also working to optimize the network traffic generated by blockchain transactions. This paper explores the application of the blockchain technology in conducting secure and transparent system for electoral voting.

III. Proposed Work

This paper proposes a blockchain based framework for electoral voting. The p2p network is backbone of the blockchain technology as the nodes in the network participates in the consensus and storing the transactions in blockchain as well.

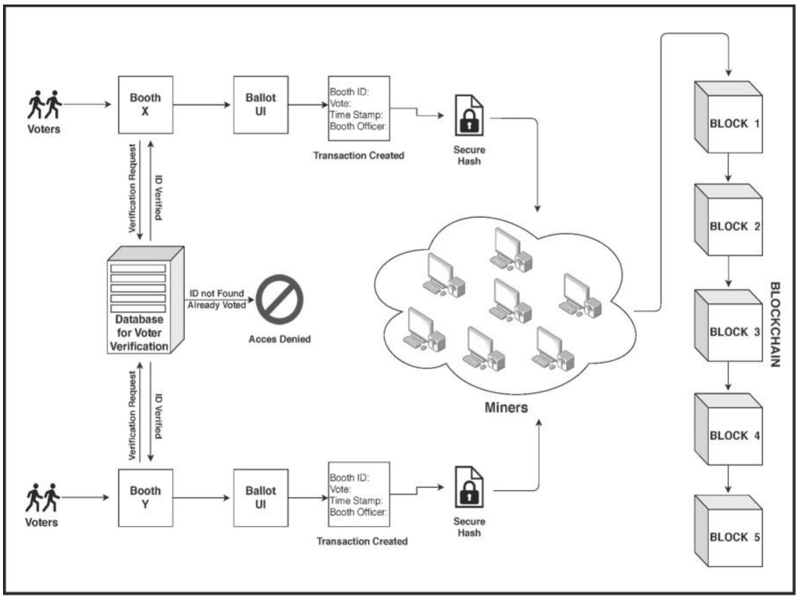


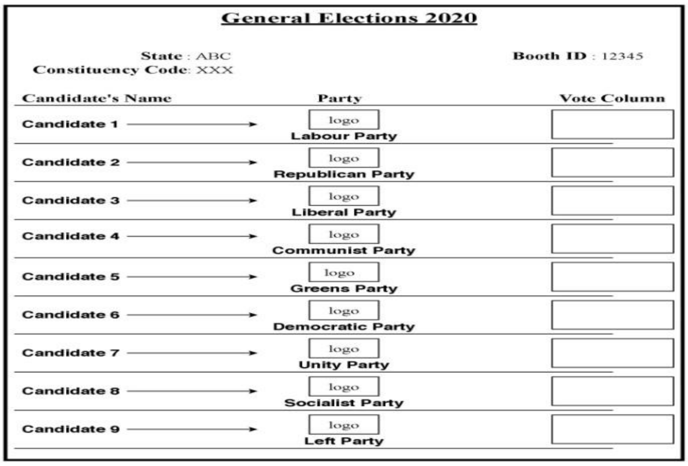
Fig. 1. Proposed Network Architecture of Blockchain Based E-Voting System

However in the proposed scenario traditional p2p network cannot be used as electoral voting process and records should be highly confidential until voting results are announced. Secondly, the privacy of the voters must be maintained in all cases. Thus, this paper proposed a type of P2P network that is composed of authorized nodes only. These authorized nodes should be authorized manually by authorities before the election. The detailed network architecture of the proposed framework is illustrated in the figure 1. In this architecture, each booth have Ballot UI interface machine that is connected to various Minors node in the network. These Minor nodes are authorized nodes. To verify the authenticity of voters each booth will have some dumb terminals connected with the centralized server of the voter's record. Access to Ballot UI machine will be granted only after biometric verification of the voters by the local authority. To conduct the electoral voting, authorities have to set such Booths across the regions. Each boot must be equipped with dumb terminals connected with centralized voter's database server, Ballot UI machines connected with minor nodes at various random locations. The each minor node maintains the complete blockchain. Conceptual working of the proposed framework is divided into two following sections:

a. Vote Casting Process
b. Vote Counting Process

Vote Casting Process

Vote Casting process describe the process of actual voting, generation of transaction and sending transactions to blockchain. In order to cast the vote, voters have to visit any booth setup by authorities. In the booth, a polling officer has to verify the authenticity of the voters be generating biometric signature and verifying the same with centralized voter's database. After successful authentication, one time access to Ballot UI machine is is granted to voters. The Ballot UI machine will have interface presenting possible options to users to cast the votes. Figure 2 describe the customizable interface of the Ballot UI machine.



General Elections 2020

State : ABC
Constituency Code: XXX

Booth ID : 12345

Candidate's Name	Party	Vote Column
Candidate 1 →	logo Labour Party	□
Candidate 2 →	logo Republican Party	□
Candidate 3 →	logo Liberal Party	□
Candidate 4 →	logo Communist Party	□
Candidate 5 →	logo Greens Party	□
Candidate 6 →	logo Democratic Party	□
Candidate 7 →	logo Unity Party	□
Candidate 8 →	logo Socialist Party	□
Candidate 9 →	logo Left Party	□

Fig. 2. Illustration of Sample Ballot UI interface

In the Ballot UI machine, voters can cast the votes by pressing the corresponding button. Each button will generate the transaction for respective votes in the background. This transaction includes SHA256 hash of the symbol of the party, Timestamp, Booth name, Booth officer id, and on which region ie, Constituency, State or Country. This transaction is added to blockchain after verification by the minor nodes. Each Ballot

UI have Digital Signature key pair (Secret key and Public key). The transaction generated by the Ballot UI machine is digitally signed by the respective secret key. The minor nodes have public key of each Ballot UI machine by which they verify authenticity of the transaction and Ballot UI. The generated transaction is explained as follows:
let parameters of vote casting transaction are defined as,

B, is the unique booth id number,

T_s, *is the timestamp,*

V_s, *is selected voting symbol by the voter ,*

V_{id}, *is voter's biometric id obtained from dumb terminal,*
hence, the each casted vote parameters is defined by set P, where all the above parameters are part of the set P except voter's biometric id.
$P = \{ B, T_s\ V_s \},$

To secure the set P, the secure hash of this set is also computed before the set P is digitally signed by Ballot UI Machine. The SHA256 algorithm is used to compute the hash of the set P.
$Hash_P \;\; = SHA256(P)$

Now, Ballot UI machine to sign the set P and hash of the set P with its secret key, hence, digital signature can be obtained using ECDSA algorithm as:
$digital\_signature = ECDSA\ (BS_K,\ Hash_P,\ P),$ *where* BS_k *and* BS_{pk} *are the Digital signature keys of Ballot UI Machine.*

Thus the final vote cast transaction is represented by set T_X as follows:
$T_X \; = \{ P,\ Hash_P,\ digital\_signature \}$

This transaction is stored in transaction pool along with the voter's bio metric id. Upon verification og the transaction and voter's bio metric id, the transaction is included into block and block is added to blockchain.
The content of block is represented by set Bl_k.
$Bl_k \;\; = \; \{ \{T_X\}_I , \{T_X\}_j , \{T_X\}_m , \ldots.\{T_X\}_n, \{V_{id}\}_l, \{V_{id}\}_k, \ldots\ldots\ldots\ldots.., \{V_{id}\}_q,\}$

The above structure preserve the voter's privacy as it is not possible to determine individual voter's casting choice. A blockchain containing such blocks is maintained by each minor in the network.

Vote Counting Process

After completion of electoral voting process, counting of votes is carried out by searching the transactions in the blockchain. To accomplish this task, blockchain from any random minor node can be used. This counting process is basically a searching process, where the hash of the symbol of each party is searched throughout the blockchain. The number of transactions in which the individual party's symbol is found is represents the total votes of that party. Figure 3 explains the complete process of counting. Using this framework, one can get information about booth wise votes, total number of votes etc. In the blockchain, once the transaction is recorded into blockchain then it becomes immutable. This property of blockchain establishes the trust of the voters in electoral system and introduce transparency in casting votes and counting of votes.

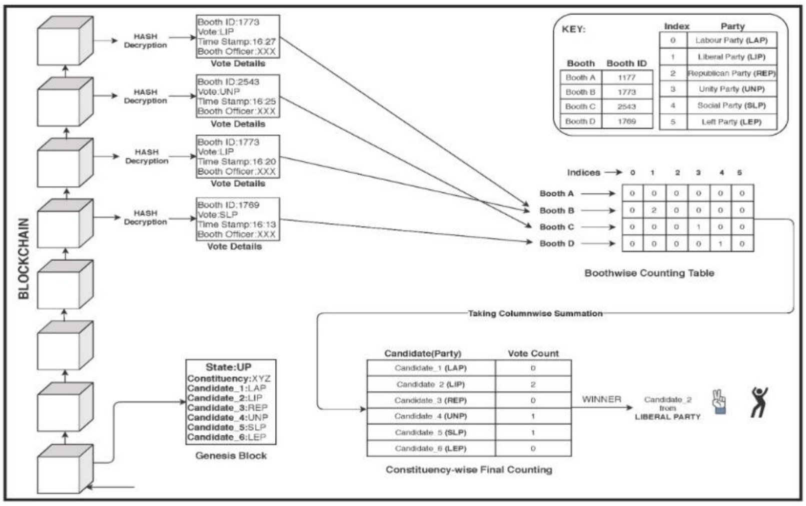


Fig. 3. Illustration of Counting of votes after electoral elections

IV. Security Analysis

In this section, a security analysis of the proposed framework is carried out. The possible vulnerability of any electoral system such as fake votes, double votes, altering the votes is discussed here.

Prevention of Fake votes

The fake vote casting or fraud voter's are the major concerns of the any electoral system. This proposed framework uses biometric based voter authentic system that can prevent fake or fraud voters to cast the votes. Hence, proposed system is not vulnerable to fake voting issue.

Prevention of Double Voting

At present, the electoral system use ink for identification voters that have cast their votes. The ink may be erased by using different types of chemicals. The proposed system keeps the records of the voter those castd their votes in blockchain. During the verification of the transaction the voter's identity is also verified by searching the voter's id in blockchain. The vote transaction is discarded in case the voter's identity found in blockchain. Thus, the proposed system is able to prevent double voting of votes by single voter.

Prevention of Vote Count Alteration

The traditional ballot paper-based election system faces issues such as booth capturing or forgery of ballot papers. The proposed system maintains the transaction in blockchain which is cryptographically secured and linked with each other. The hijacking or alteration is not possible in this system.

V. Conclusion

This paper proposes a novel framework for electoral voting system. This system offer flexibility to voters to cast the votes from any booth unlike dedicated booth in traditional voting system. The use of blockchain technology in this framework establishes the trust, transparency and ease of voting. This paper also discusses the handling of general challenges of electoral voting system. This proves that proposed system is not vulnerable to the issues such as fake voting, multiple voting by single voter and alteration of the vote count. The robust framework transforms the EVM based voting system to the one level up in terms of the efficiency and scalability. However, there exist some limitations of maintaining the network of minor nodes and network connectivity of each booth with the blockchain network. These limitations are not major issues as the most of the countries are developing their IT infrastructure rapidly.

Conflicts of Interest:

The authors declare that they have no conflicts of interest regarding the paper.

References

I. Eastlake 3rd, D., Jones, P.: US secure hash algorithm 1 (SHA1). (2001).

II. Ferrer, E.C.: The blockchain: a new framework for robotic swarm systems. arXiv Prepr. arXiv1608.00695. (2016).

III. Foundation, Po.et - proof of existence on the top of bitcoin blockchain, https://www.po.et, last accessed on August 13, 2018.

IV. Herbert, J., Litchfield, A.: A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology. In: Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015). p. 30 (2015).

V. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published Pap. August. 19, (2012).

VI. Lemieux, V.L.: Trusting records: is Blockchain technology the answer? Rec. Manag. J. 26, 110–139 (2016).

VII. Litchfield, A., Herbert, J.: ReSOLV: Applying Cryptocurrency Blockchain Methods to Enable Global Cross-Platform Software License Validation. Cryptography. 2, 10 (2018).

VIII. Mallick, S., Pandey, R., Neupane, S., Mishra, S., Kushwaha, D.S.: Simplifying Web Service Discovery & Validating Service Composition. In: Services (SERVICES), 2011 IEEE World Congress on. pp. 288–294 (2011).

IX. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008).

X. Shiela David, R. Aroul Canessane. : 'FOOD SAFETY USING RFID TAGS IN BLOCKCHAIN TECHNOLOGY'. *J. Mech. Cont. & Math. Sci., Vol.-15, No.-8, August (2020) pp 299-306*. DOI : 10.26782/jmcms.2020.08.00028.

XI. Underwood, S.: Blockchain beyond bitcoin. Commun. ACM. 59, 15–17 (2016).

XII. Yogesh Sharma, B. Balamurugan. : 'A SURVEY ON PRIVACY PRESERVING METHODS OF ELECTRONIC MEDICAL RECORD USING BLOCKCHAIN'. *J. Mech. Cont.& Math. Sci., Vol.-15, No.-2, February (2020) pp 32-47*. DOI : 10.26782/jmcms.2020.02.00004.