International Journal of Current Engineering and Technology
©2021 **INPRESSCO**®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Application of BCT in Secure Electronic Voting System

Sharad Poman and Dr. G.M. Bhandari

Dept of Computer Engineering, BSIOTR, Pune, India.

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

This Millennial has brought in increasing use of technologies related to revolutionized life of people. Digital World has its hand in every aspect of system where use of paper was implemented. Electrol voting system is one of this where digitization is majorly used. With digitization, aspect of security and privacy becomes threat for conventional system(offline), Keeping the same in mind centralized system was introduced where only one organization was able to manage whole system. But with this also tampering of database and votes can be done. Thus, we have introduced Block chain technology which is one of solutions, as it embraces a decentralized system and the entire database are owned by many users. Decentralized Bank System use blockchain technology which is form of the Bitcoin system. By implementing the same block chain technology in the distributed databases on e-voting systems one can reduce the unfair manipulation of databases. This paper aims to implement e-voting using blockchain technology to give result from each individual place of election, thus to give voting result with more transparency and authority.

Keywords: *blockchain, e-voting, security, network security.*

1. Introduction

Block Chain Technology is latest on list to give secure and transparent results for any application utilized. E-voting is one application where appropriate use of blockchain can be done. This also focuses on use of database for covering and recording. The system which is built can be built upon used bitcoin nodes. These nodes are independently random and not counted. Blockchain permission is made compulsory to change from bitcoin to blockchain node, as these nodes are the main point of contribution as registered place of voting in general elections. Thus, earlier to implementation, it must be clear about the amount and the identity. Data Integrity is maintained with this method which restricts manipulation that might happen during election process. When voting process takes place and is completed at each node, the process of data integrity and security begin. Before the election process begins, each node generates a private key and a public key. All nodes in list of election process receive Public Key. After the election process is done, election result is collected from each individual node as per every voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then verification is done to determine whether the block is valid. Once validity id checked, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into block- chain. The submitted block contains the id node, the next id node as used as the token, time stamp, voting result, previous node HASH, and the digital signature of the node. The block-chain technology with block containment of the smart contracts, can be put to use in developments of easy to use e-voting system. Block Chain is safer, cheaper, more secure, and more transparent. In the proposed system we solve existing following problems like that of transparency, authentication and provability in the voting platform.

The system need to see that the people who attend the elections are real people and use correct credentials that we know in electronic environments, and we should be able to prove that any time, also we need our elections are 100% transparent as desired. So, we need to gather and check signed and time stamped data of the elections. Because, nobody should be able to change the votes after they are casted. Also, we need individuality in elections, so that nobody can vote for someone else.

Literature Survey

1. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System

The paper is a version of peer to peer transaction of payment electronically to be directly send from one customer to different without interference of going through financial institute. Part of solution is provided by use of digital signature but main use is lost when the third party is needed to prevent double spending. A solution to double spending problem in peer to peer network is resolved by author in his paper. The transaction are timestamped by network by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, the transactions generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone[1].

1. **Christopher D. Clack, Smart Contract Templates**:

The foundations, design landscape and research directions. In this position paper, authors consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agreement whose execution is both automatable and enforceable. They have explored a simple semantic framework for smart contracts, covering both operational and non-operational aspects. Authors describe templates and agreements for legally-enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, authors identify operational parameters in the legal documents and use these to connect legal agreements to standardized code. The authors also explore the design landscape, including increasing sophistication of parameters, increasing use of common standardized code, and long-term academic research. Authors conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates [2].

2. **Epp Maaten, Towards remote e-voting**:

This paper gives an overview about the Estonian evoting system. Paper discusses how the concept of evoting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.[3]

3. **Paul Gibson, A review of E-voting:**

The past, present and future, Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades[4].

4. **Muhammad Ajmal Azad, M2M-REP:**

Reputation of Machines in the In- ternet of Things 2017. The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collabora- tive reputation system that calculates trustworthiness of machines in the IoT- based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this paper presents a novel M2MREP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way[5].

5. **Kashif Mehboob Khan Secure Digital Voting System based on Blockchain Technology**:

Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as in- creased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to im- proving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e- voting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for evoting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multichain platform. The paper presents in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme[6].

Proposed Methodology

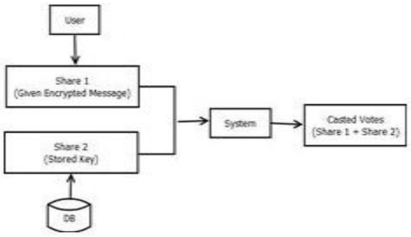


Fig: System Architecture

Algorithm

1) **AES (Advanced Encryption Standard)**

The Advanced Encryption Standard, or AES, is a symmetric block cipher to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. It is applied, along with other operations, on an array of data that holds exactly one block of data, this block is encrypted with help of round keys.

This array we call the state array.

STEPS: Derive the set of round keys from the cipher key.

- ➢ Initialize the state array with the block data (plaintext).
- ➢ Add the initial round key to the starting state array.
- ➢ Perform the tenth and final round of state manipulation
- ➢ Copy the final state array out as the encrypted data (ciphertext).

2) **MD5: Hash Function**

Step 1. **Append Padding Bits.**

Length of message (in bits) is congruent to 448, modulo 512 as the message is Padded.

Step 2. **Append Length.**

Step 3. **Initialize MD Buffer.**

Step 4. **Process Message in 16-Word Blocks.**

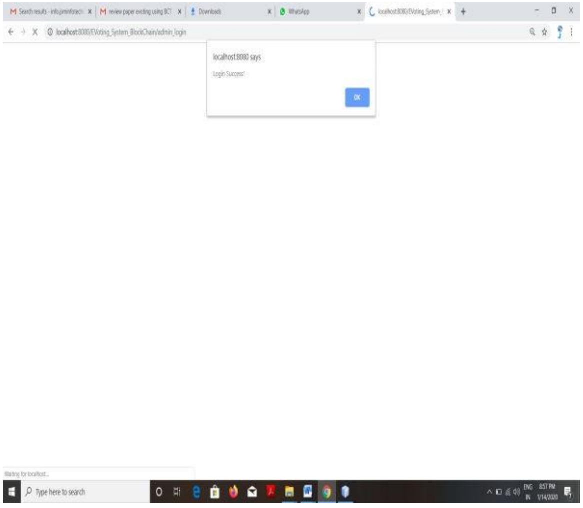
Step 5. Output.

Cryptographic hash function with 128-bit hash value is widely used as MD5 Algorithm in cryptography.MD5 is Message-Digest algorithm 5.

MD5 is used in security application to check the integrity of files. It is expressed as 32-digit hexadecimal number.

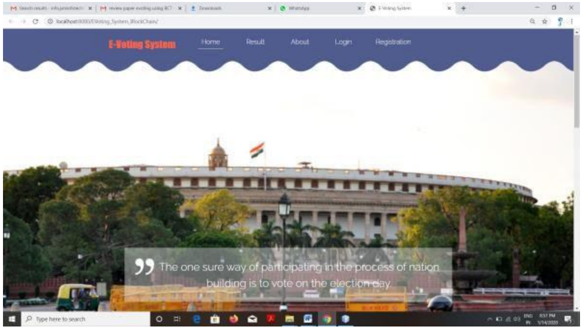
Results and Discussion

Figure 1 to Figure 6 shows the partial work completion towards the whole system of e-voting. The work completed till now shows the Admin panel (Figure 3), procedure to add candidate for voting in Figure 4. Participated candidates are viewed as according to Figure 5. Then the procedure to register individual user is shown in Figure 6.


localhost:8080 says

Login Success!

Fig 1: Home Page



The one sure way of participating in the process of nation building is to vote on the election day.

Fig 2: Admin Login Success

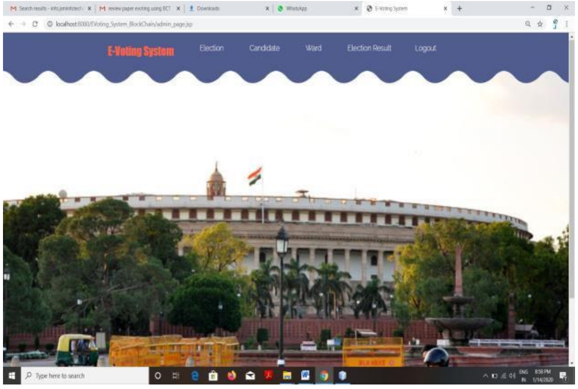
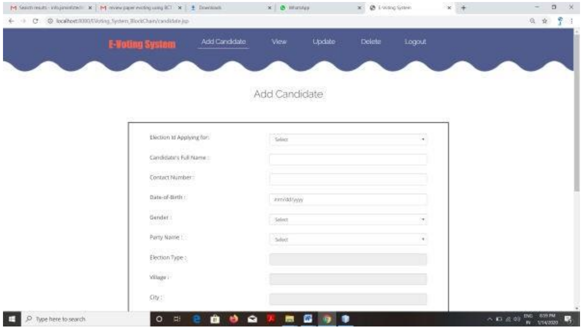


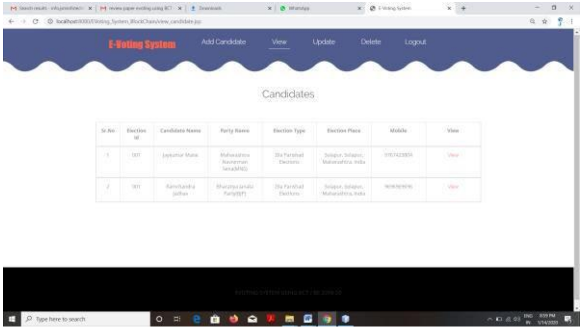
Fig 3: Admin Home



Add Candidate

Election Id Applying for: Select
Candidate's Full Name :
Contact Number :
Date-of-Birth : mm/dd/yyyy
Gender : Select
Party Name : Select
Election Type :
Village :
City :

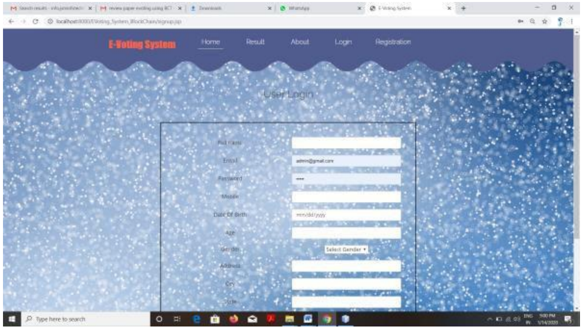
Fig 4: Admin Add Candidate



Candidates

Sr.No	Election Id	Candidate Name	Party Name	Election Type	Election Place	Mobile	View
1	001	Jaykumar Mane	Maharashtra Navnirman Sena(MNS)	Zilla Parishad Elections	Solapur, Solapur, Maharashtra, India	[illegible]	View
2	001	Ramchandra Jadhav	Bharatiya Janata Party(BJP)	Zilla Parishad Elections	Solapur, Solapur, Maharashtra, India	[illegible]	View

Fig 5: Admin View Candidate



User Login

Full name	
Email	admin@gmail.com
Password	****
Mobile	
Date Of Birth	mm/dd/yyyy
Age	
Gender	Select Gender ▾
Address	
City	
State	

Fig 6: User Registration

Conclusion

Choosing a right leader for nation is very important when the dependency is on number of votes cast by citizens of nation. Citizens struggle to cast vote which can be maintained secret and trustworthy. In democratic voting, to have secure data with trustworthiness among the people is essential, this is obtained with the system we have proposed, to cast votes through E-voting. Through application in decentralized Bank system, Block chain technology is itself technology to give secure data and avoid cheating through database manipulation. Thus, this project has aimed to implement E-voting using Block Chain technology and algorithm to give secure and trustworthy result.

References

[1]. Rifa Hanifatunnisa, Budi Rahardjo, Blockchain Based E-Voting Recording Sys- tem Design,IEEE 2017[2].

[2]. Design a Secure Voting System Using Smart Card and Iris Recognition, Md. Mahiuddin Department of Computer Science and

[3]. Engineering, International Islamic University Chittagong (IIUC), Chittagong, Bangladesh, 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)

[4]. Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and Its Applications A Detailed Survey, International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017[5].

[5]. SHARVOT : secret Share based voting on the blockchain,Silvia Bartoluccinchain,London,Uk,IEEE 2018 Asraful Alam, S.M.Zia Ur Rashid,Towards Blockchain Based E-Voting System,2018 IEEE[4].

[6]. Rabeya Bosri , Abdur Razzak Uzzal , Towards A Privacy Preserving Voting System Through Blockchain Technologies , IEEE 2019

[7]. Design a Secure Voting System Using Smart Card and Iris Recognition, Md. Mahiuddin Department of Computer Science and

[8]. Engineering, International Islamic University Chittagong (IIUC), Chittagong, Bangladesh , 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)

[9]. Secured and transparent voting system using biometric ,2018 2nd International Conference on Inventive Systems and Control (ICISC) ,Ch. Jaya Lakshmi(Dept. of EIE V.R. Siddhartha Engg. College Vijayawada) , S. Kalpana (Dept. of EIE

[10]. V.R. Siddhartha Engg. College Vijayawada Teja K , Shravani MB , Secured voting through Blockchain technology , 2019 IEEE

[11]. Cosmas Krisna Adiputra , Rikard Hjort and Hiroyuki Sata , A proposal of Blockchain Based Electronic Voting System , IEEE 2018