Volume 4 || Special Issue 7 || ICCEME 2019-2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

# A STEP TOWARDS DIGITAL VOTING SYSTEM USING BCT

**Poman Sharad[1], Dr. G. M Bhandari[2]**
*Department of Computer Engineering, Savitribai Phule Pune University, Pune, India.*

**Abstract- Increasing digital technology has revolutionalized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions, because it embraces a decentralized sys- tem and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.**

## I INTRODUCTION

The block-chain technology used mostly works the same as the blockchain technology contained in the E-voting system and focuses on database recording. The nodes involved in Blockchain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a blockchain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each 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 done verification to determine whether the block is valid. Once valid, 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 block-chain 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, hash of the previous node, and the digital signature of the node. The block-chain with the smart contracts, emerges as a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e- voting systems. In the proposed system we solve existing following problems solve. We need transparency, authentication and provability in the voting platform. We need to assure 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.

## II LITERATURE SURVEY

1. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions 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, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Mes- sages 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.

2. Christopher D. Clack, Smart Contract Templates: foundations, design landscape and research directions. In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automa- tion, enforceability, and semantics) and define a smart contract as an agree- ment whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non-operational aspects. We describe templates and agreements for legally- enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, we identify operational parameters in the legal docu- ments and use these to connect legal agreements to standardised code. We also explore the design landscape, including increasing sophistication of parame- ters, increasing use of common standardised code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

3. EppMaaten, Towards remote e-voting: Estonian case This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting 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.

4. 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 pro- cess. Electronic voting has been deployed in many different types of election throughout the world for several decades.

5. 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 pa- per presents a novel M2M-REP (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

6. KashifMehboob 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 improving 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.

## III PROPOSED SYSTEM

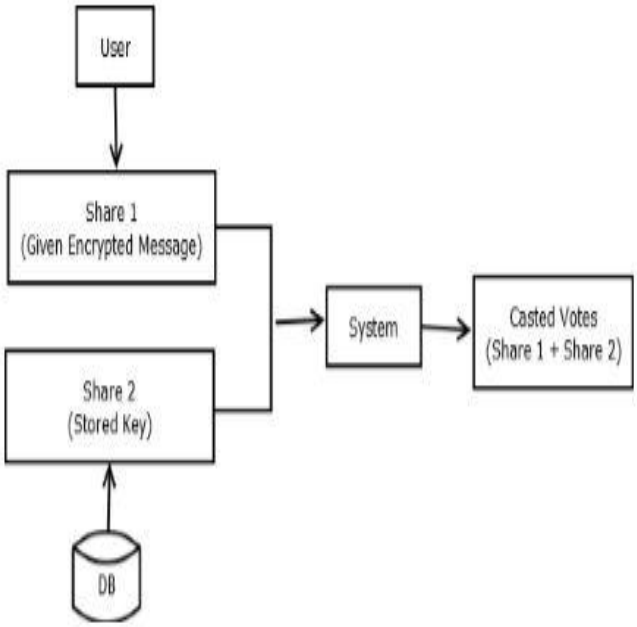


***Figure 1 System Architecture***

**Algorithm:**

AES is used to encrypt the database.
The encryption process uses a set of specially derived keys called round keys.
These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted.
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).

MD5: Hash Function
Step 1. Append Padding Bits. The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. ...
Step 2. Append Length. ...
Step 3. Initialize MD Buffer. ...
Step 4. Process Message in 16-Word Blocks. ...
Step 5. Output.
In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value.
As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.
An MD5 hash is typically expressed as a 32 digit hexadecimal number.

## IV EXPERIMENTAL RESULTS:


*Figure 2: Home Page*

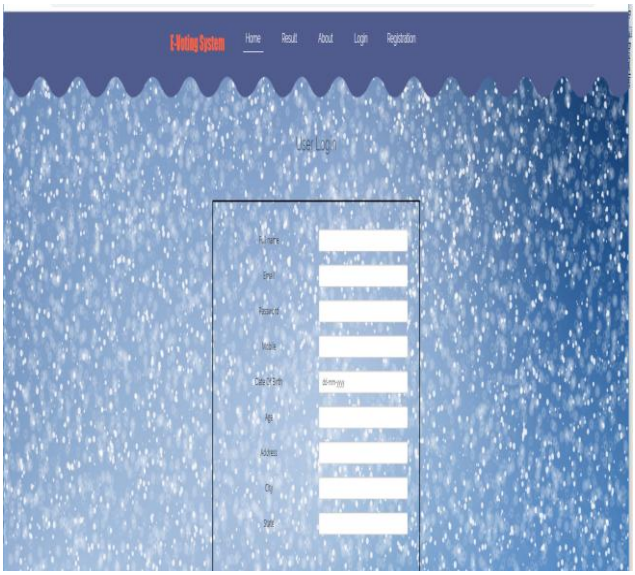


*Figure 3: Registration*


*Figure 4: Visual Cryptography*

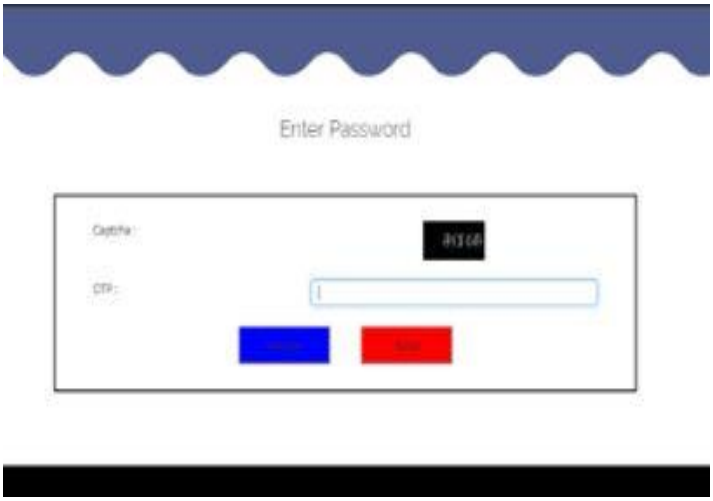


*Figure 5: Visual Cryptography*


***Figure 6: Result***

## V CONCLUSION:

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

## REFERENCES

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

[3] 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].

[4] 4.SHARVOT : secret Share based voting on the blockchain,Silvia Bartoluccinchain,London,Uk,IEEE 2018

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

[8] 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 V.R. Siddhartha Engg. College Vijayawada

[9] Teja K , Shravani MB , Secured voting through Blockchain technology , 2019 IEEE .

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