International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 1473–1478

Application Of Bct In Secure Electronic Voting System

Prof. P.T. Suradkar, Mayur Mandlik, Gayatri Kothawade, RutujaAndhalkar,

Anjali Jagtap

Department of Computer Engineering, NBNSSOE, Pune

Abstract

As traditional election uses electronic devices which needs paper for its working. Also we are not sure about the security and transparency which may be a threat. Currently traditional election uses centralized system whose database and system is controlled from one organization. This may cause occurrence of many issues if the system fails. Database if gets hacked may cause long time for recovery and can hyper all the organization at the same time. But block chain election system has control of all the database from its specific organization so if system fails can cause issue to one organization and others can work without any trouble. Also block chain reduces the chances of security break as the database goes one level lower in size more secured it can be made. Block chain itself has been used in the Bit-coin system consulted to as the decentralized Bank system. The ultimate aim of project is to represent the voting result using Block Chain that too from every place of election. Unlike Bit-coin with its Proof of labor, this can be a way supported a predetermined activate the system for every node within the built of block chain.

I. INTRODUCTION

E-voting System using Block chain mainly focuses on database recording same as block chain technology works in most of the technologies. The Block chain nodes concerned in Bit-coin are severally random and not counted. This method mainly focuses on data integrity that is data is protected from manipulation which is the main key of any election process. This process is evokedwhen voting process at each node has been finished. Prior of Election process, each node generates private key and public key. Public key of each and every node is send to all the nodes listed in election process, so that each node has public key of all nodes. When the election process occurs, each node collects results from each voter. After completion of election process, nodes willhold for their turn to generate block. After appearance of block at each node, validationis done to determine whether block is valid or not. If true, the database will then be modified with the block data. After the database has been modified, the node checks whether or not the node ID brought as token are his. If the node gets a turn, a block filled in with a digital signature will be generated and sent for broadcast to all nodes by using turn rules in block-chain formation to avoid collision and to ensure that all nodes join the block-chain.The submitted block includes Id node, next Id node used as a token, time stamp, vote count, previous node hash and node digital signature.The block chain having smart contracts emerges pretty much as good candidate in development of secure, safer, easier to use and more transparent electoral system. During this proposed system we solved the majority existing system problems. We'd like provability, transparency and authentication in voting platform. We wanted to assure that the folks that attended elections are real and use correct credentials that we all know in electronic environments and that we should be ready to prove it any time. Also we'd like to assure that elections are 100% transparent as desired. So, we'd like to test time stamped and signed data of the elections in order that nobody should be ready to change votes once casted. Also we'd like individuality in election in order that nobody castes somebody else vote.

ISSN: 2233-7857 IJFGCN

II. LITERATURE SURVEY

1. Satoshi NakamotoBitcoin: A Peer-to-Peer digital cash device. Abasic terms peer-to-peer model of digital coins could permit on-line payments to be dispatched at once from one celebration to an extraordinary without gaining knowledge of a group. Digital signatures offers a part of the answer, but the most advantages are misplaced if a relied on third party remains required to forestall double-spending. We propose an answer to the double-spending problem using a peer-to-peer network. The community is such that it records time and date of transaction by means of hashing them right into a non-stop chain of hash based proof-of-work, which will in the end shape a document that may not be modified without redoing the evidence of labor. The longest chain now not best is evidence of the collection of events witnessed, however evidence that it came from the maximum important pool of CPU power. The bests of first-rate efforts have been taken for message broadcasting and the gadget is such that nodes can leave and rejoin the community at will and the proof of whilst they have been gone the longest evidenceof chain is accepted.

2. Christopher D. Clack, Smart Contract Templates: Foundations, layout panorama and studies directions. We don't forget foundational subjects consisting of terminology, automation, enforceability etc. Regarding smart controls and outline an agreement which can be each automatable and enforceable.A smooth semantic framework for smart contracts, covering each operational and non-operational aspect was explored. We define templates and agreements for clever
Contracts legally enforceable, and endorse criminal documents.We perceive operational parameters while constructing upon the Ricardian Contract Triple within the prison documents. Standardizes code are used to attach those documents. Exploration of look landscape which includes growing complexity of parameters, growing use of commonplace standardized code and longtime academic studies.We conclude through identifying more paintings and setting forth an initial collection of necessities for a well-known language to aid Smart Contract Templates.

3. EppMaaten, toward far flung e-vote casting: Estonian case this paper offers an outline approximately the Estonian e-voting gadget. The paper attempts to shower upon a number of selections regarding easy functioning of e-vote casting in particular resisting the demanding situations of faraway e-balloting, giving the risk of re-vote, and the manner an e-vote casting gadget might be made comprehensible to make the general public accept as true.

4. Paul Gibson, An overview of E-vote casting: The past, present and destiny Electronic voting systems are the ones which depend upon a few electronic technologies for his or her correct functionality. Many of them rely on such era for the verbal exchange of election data. Relevance verifiability, dependability, security, anonymity and accept as true with are some of the technical demanding situations faced at some point of elections. Changing the manner in the course of which humans vote has many consequences for culture and politics.The function of election directors and observers is fundamentally different because the process involves complicated technology. Electronic voting has been used for many decades in several alternative varieties of elections across the globe.

ISSN: 2233-7857 IJFGCN

5. M. A. Azad, M2M-REP: Reputation of Machines inside the web of Things 2017. The trap of Things (IOT) is that the mixture of an outsized number of self-ruling heterogeneous gadgets that report data from the healthiness to the observing framework for examination and significant choices. The undermined machines inside the IOT system might not exclusively be utilized for spreading undesirable substance like spam, malware, infections so forth., however may report falsehood about the physical world which will have an appalling result. The test is to style a collective notoriety framework that ascertains reliability of machines inside the IOT-based machine-to-machine arrange without expending high framework assets and rupturing the safety of members. To cope with the test of protection safeguarding notoriety framework for the decentralized IOT condition, this paper presents a completely special M2M-REP (Machine to Machine Reputation) framework that figures worldwide notoriety of the machine by amassing the scrambled nearby input gave by machines in an exceedingly completely decentralized and confirm about way.

6. K.M. Khan Secure Digital legitimate framework bolstered Blockchain Technology. Electronic democratic ballot has been utilized in alternating structures since 1970s with some major advantages over paper-based frameworks like growth in productivity and deduction in mistakes. In any case, there remain difficulties to acknowledge wide spread appropriation of such frameworks particularly with significance improving their versatility against potential flaws. Square chain can be a difficult innovation of current time and vows to support the strength of e-casting a ballot framework. This paper presents a preliminary to use advantages of blockchain like cryptographic establishments and incomplex to understand a proficient plan for e-casting a ballot. The proposed conspire fits in with the natural prerequisites for e-casting a ballot plots and accomplishes start to finish undeniable nature. The paper presents subtleties of the proposed e-casting a ballot conspire together with its execution utilizing Multichain stage. The paper presents top to bottom assessment of the plan which effectively exhibits its adequacy to understand a start to finish evident e-casting a ballot conspire.

III. PROPOSED METHODOLOGY

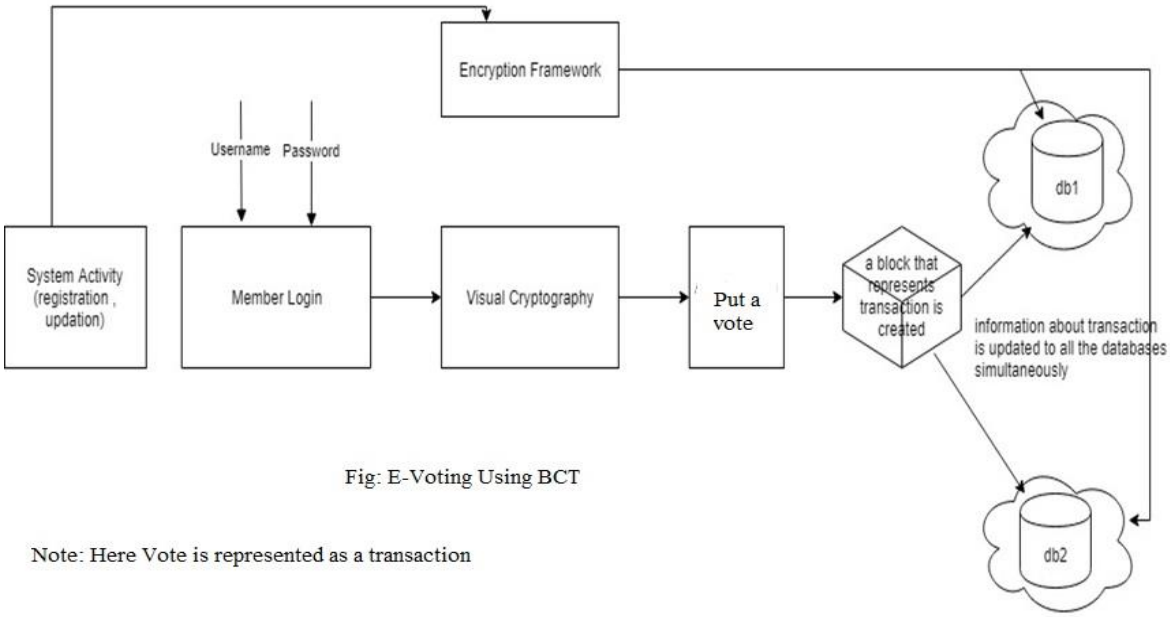

Fig: E-Voting Using BCT

Note: Here Vote is represented as a transaction

Algorithm:

ISSN: 2233-7857 IJFGCN

To encrypt the database AES is used.

Round keys which are specially derived set of keys are also used for encryption process.

The data which is to be encrypted on array of data that holds exactly unit block of data which applied along with some other operations.

The different name of this array is 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, cryptographic hash function with a 128-bit hash value is used which is MD5.

According to Internet standard (RFC 1321), the integrity of files is also checked by MD5 algorithm.

An MD5 hash is usuallyconveyed using a 32 digit hexadecimal number.

III. RESULTS AND ANALYSIS

	Traditional Elections	**E-voting System using Block chain**
Strengths	1. As long as process is transparent, people belief the paper based voting and counting. 2.Good for regions with low internet existent if does not trust on internet and computers.	1.Unchangeable records. Deletion of records is nearly not possible; evenif it is fortunate, the proof of deletion can be prevented. 2.It provides privacy with transparency. 3. In the long term it is cheaper. 4. Itenables flexible elections inconsistent durations,target groups and conditions. 5.Provides results immediately.

ISSN: 2233-7857 IJFGCN

Weakness	1.In the long term costs are extremely high. 2.With the presence of person it may tough and annoying. 3.Physical safety is costly and tough. 4.Not possible to place vote centers in small-scale and long away settlements. 5.For terrorism crowded vote centers become open targets.	1.The strengths will depend onexecution. 2.There are some scalability issues as technology is newly discovered. 3.On high usage the performance may degrade. 4.Developer and testing tools are not adequate; Insufficient tooling.
Opportunities	1.For smaller and non-distributed groups it is easier and cheaper.	1.To improve voting transparencies provides new solutions. 2.Secured voting and remote participation. 3. Storage and records are Secure. 4.Once this system is learned it is easier for aged and disabled persons. 5.Might bring more democracy to Government section, local management.
Threats	1.During counting errors may cause by human-factor. 2.The voting process may distort or block by physical attacks. 3.In case of appeals, re-holding elections are extremely expensive. 4.Complications regarding holding election may result in having reduced election.	1. Attackers can abuse the system, if the Cryptographic keys are compromised.

V. CONCLUSION

Use of e-voting using BCT is secured, transparent and user friendly. It can reduce existing issues which are faced by traditional voting system. As the system is decentralized, the problem of corruption will be resolved and people will get their leader by majority. So traditional voting system can get easily replaced using e-voting application.

REFERENCES

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

ISSN: 2233-7857 IJFGCN

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, VrushaliKulkarni, Blockchain and Its Applications A Detailed Survey, International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017[5].
4. SHARVOT : secret Share based voting on the blockchain,SilviaBartoluccinchain,London,Uk,IEEE 2018
5. AsrafulAlam, S.M.Zia Ur Rashid,TowardsBlockchain Based E-Voting System,2018 IEEE[4].
6. RabeyaBosri , AbdurRazzakUzzal , 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. TejaK ,Shravani MB , Secured voting through Blockchain technology , 2019 IEEE .
10. CosmasKrisnaAdiputra , RikardHjort and Hiroyuki Sata , A proposal of Blockchain Based Electronic Voting System , IEEE 2018

ISSN: 2233-7857 IJFGCN