Blockchain-based E-Voting System using Proof of Voting (PoV) Consensus Algorithm

S. Srinivas[1], B. Ashwin Kumar[2] and R. Srishylam[3]
[1] Asst. Professor, CVR College of Engineering/CSE Department, Hyderabad, India
Email: s.srinivas@cvr.ac.in
[2] Asst. Professor, CVR College of Engineering/CSE Department, Hyderabad, India
Email: forashwink@gmail.com
[3]Asst. Professor, CVR College of Engineering/CSE Department, Hyderabad, India
Email: srisailamreddypally@gmail.com

Abstract: **Designing the Electronic Voting System is the biggest challenge, especially in India. It has to satisfy all the legal guidelines and have a robust tamper proof system. E-voting system can be made up of central and distributed network types, but the main disadvantage of central network is single point of failure. Blockchain technology is a distributed type of network many applications like Electronic medical records (EMR), IoT and E-voting. In this paper an electronic voting system using blockchain technology with powerful Proof-Of-Voting (POV) consensus algorithm is developed. This paper evaluates the legal issues that are encountered in conventional methods and how to overcome them with the help of blockchain technology. In this paper one system has made with PoV which increases security, is of low cost and low power consumption.**

Index Terms**: Blockchain Technology (BCT), Electronic Voting (E-Voting) , Proof-of-voting (POV).**

I. Introduction

In early 80's and 90's some countries used traditional pen and paper method for the conduction of general elections. [1,2,3], Traditional method of conducting elections had many challenges like rigging, booth capturing and misleading the results. There was no proper mechanism to conduct free and fair elections. Many studies were conducted to overcome these issues. E-Voting System [4] is the most authentic and accurate method and good solution for conducting fair elections in the democratic countries. Now a days many countries are using E-voting systems with a micro controller, required software with the program designed for the purpose . There is every possibility to tamper or hack the system because of central accessible storage. This may affect the election results. This paper shows implementation of E-voting system with blockchain Technology taking into consideration national security, utilization of efficient man power and minimizing fraud. The mechanism can be effective if:

1. Voter information and vote casting should keep in secret.
2. Voter id verification and count of votes have to be correct.
3. No other person should not tamper the vote.

Blockchain is a digital trust with decentralized, digitized, public and shared ledger of information that is resistant to tampering. The main features of blockchain [5,6] technology is;

1. Enhanced security features, preventing fraud and data theft.
2. Improve the overall robustness and integrity.
3. Securing edge devices with authentication and data management.
4. Reduce the fishing attacks, DDoS (Distributed denial of service) attacks.

With these features of cryptography, every node in blockchain is linked with hash pointer, verified signed transactions are replicated globally on millions of nodes. For these reasons and features now 33% of organizations are using blockchain technology.

Section II gives the information about Blockchain as a service for E-voting. Section III describes proof of vote consensus mechanism. Section IV describes security analysis proposed consensus algorithm. Section V describes conclusion and future scope.

II. Blockchain as a Service for E-Voting

In this section it is considered that E-Voting system is based on blockchain technology. Firstly, in this section will be discussed about how to create smart contacts, next about different frameworks in blockchain then how to deploy election using smart contacts and in last about the proposed system.

A. Creating Election Smart Contacts

Smart contacts [7] include identifying the roles that are involved in election like voter, officer, nodal officer. There are different election roles can be made as smart contacts. Figure 1 shows the participants in E-Voting system and how election will be initiated. Firstly, election administrator starts the election and after particular time he closes the election, total election process monitored by election administrator. Next district officer having the information about next sub level like district-wise, next booth officer to the voter last. Booth officer will be in the polling booth and he monitors the election of single polling booth. Smart contacts created for all of them in the network from administrator to voter. To cast vote every node has to make authentication. So that it will give perfect result and no other persons can tamper the network.

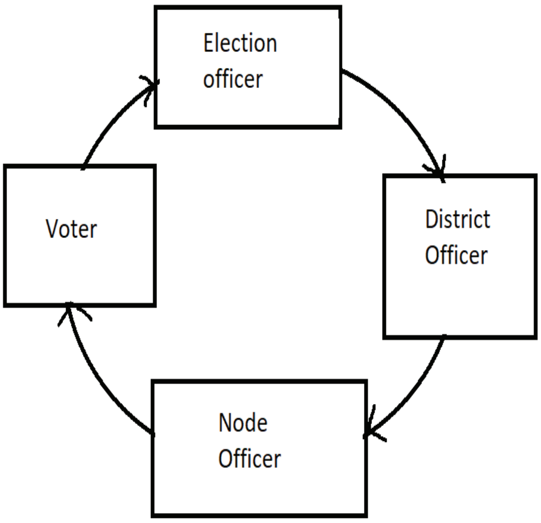

Figure 1. Election process initiation using smart contacts

B. Election Procedure

Election officer creates decentralized application for election procedure. Main activities of election process using blockchain technology [14,15,16] are election creation, voter registration, voter transaction, tallying results and verifying vote. Figure 2 shows how the election process done using proof of vote network [17].

A new consensus method permissioned Proof of voting [8,9] is proposing here. After initiating election process election starts with candidates list and smart contacts of every candidate. Each ballot smart contact created by node officer to particular candidate and it is verified by district and node officer. Voter registration made by using proof of vote (POV). If the candidate's smart contact is matching with the ballot smart contact then only voter can cast his vote, if he fails in this process then voter is not allowed to cast his vote. The same work can be done using proof of work (POW) [10,11] also, but the power consumption is very high in POW where as in POV the power consumption is low. Next session will give the information about POV consensus mechanism [18,19]. After verification done, tally of votes and voter transaction can be done by conventional methods.

III. Proof of Voting (PoV) Consensus for E-Voting System

Consensus is important concept in block chain technology. Block Chain Technology (BCT) is a distributed technology so that anybody can enter in to the network if it is permission less BCT. Every node and process have to maintain same data and understanding. In permissioned BCT all nodes are known to each other where as in permission less BCT nodes [20] are unknown to each other. Some malicious nodes may not follow the consensus due to that voting data may get leaked.

In this paper the analysis made on byzantine agreement and smart contacts.

Byzantine agreement: it is an agreement between every node in the network that they stand up on same rules. If any of the node is not following the rules then that node is called as malicious, such nodes will be removed from network. If the malicious nodes are increasing and agreement between the nodes are break means that called byzantine failure.

Smart contacts: is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions. A smart contact works in the same way as a traditional contact while also automatically enforcing the contact.

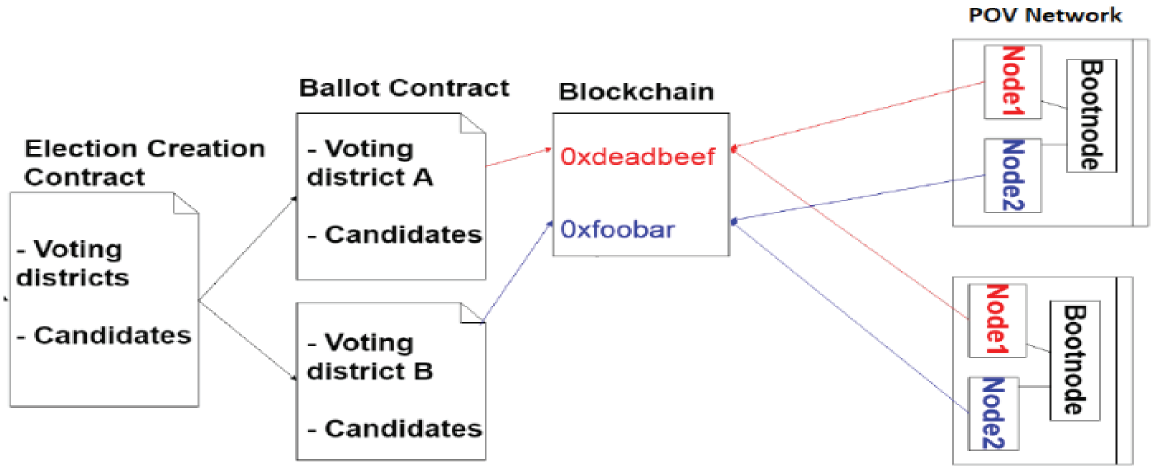

Figure 2. Election procedure using smart contacts

In this proposed consensus [12] algorithm, it will predict the malicious nodes and removes it from the Block Chain. In E-voting system it is important to remove some failures like byzantine failure [13], security failure, crash failure, software failure and temporal failure. Figure 2 shows how the consensus achieved in distributed system. In block chain if any of the node is behaving like malicious (attacker) then automatically detected by proof of vote (PoV) algorithm and those attackers will be removed from block chain.

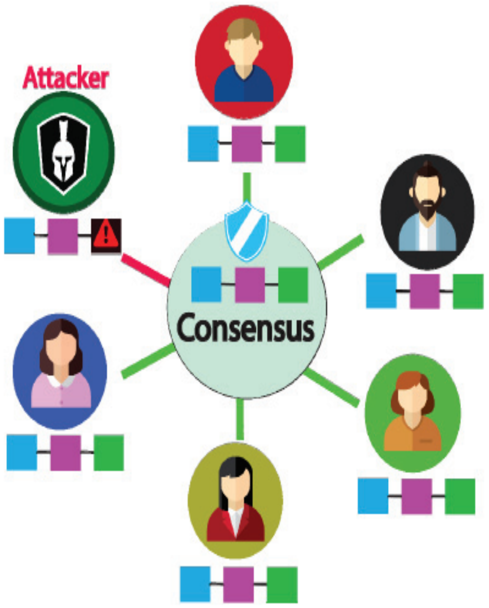

Figure 3. consensus in proof of vote (PoV)

A. Mathematical Model For POV

In Proof of voting consensus algorithm, blockchain systems are maintained by various enterprises around the world or country. Applications developed on this network can serve terminal users across the world. The network model for POV is shown in figure 4. There are four following roles in POV consensus process: commissioner, butler, butler candidate and ordinary user.

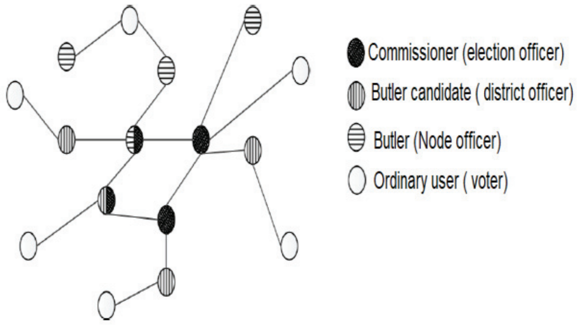
● Commissioner (election officer)
◍ Butler candidate (district officer)
⊜ Butler (Node officer)
○ Ordinary user (voter)

Figure 4. Proof of voting network model

Commissioner: several voters from different parts of the country are formed league committee, commissioner is one of the members in league committee. In this paper commissioner is considered as election officer. Commissioner has the right to recommend, vote and evaluate the voter. A block is generated in blockchain network will be sent to all election officers for verification. When the block has received 51% votes from all commissioners then the block is considered as valid block and added to the blockchain.

Butler: Butler is responsible for producing blocks. The identity of the butler means the separation of a voting right and an executive right. The function of the butler is to transact the information from the network gathered by it and pack the information with the block. Node officer's responsibility is same as butler's responsibility.

Butler candidate: He is the responsible for the communication between node officer and voter. In our case butler candidate and district officer both are same. Butler candidate gathers the information of voter and if it matches with the network then checks the number of votes in the network, if the majority of networks are find then voter is marked as authenticated.

B. Voting Process

Two steps involved in voting procedure. Voting for the block production and voting for the candidate. The commissioners vote by returning their signature. In this analysis, it is assumed that N_c- number of commissioners, N_b- number of butler candidates, N_{bc}- number of butler and N_v- number of voters.

Voting for block production: Butler *i* generates a block and sends it to all commissioners. If a commissioner agrees to produce this block, he will encrypt the block header and returns the signature to butler *i*. If butler *i* receives at least $N_c/2 + 1$ signatures within the predefined time, the block is valid. Otherwise, the block is invalid, and will be reproduced by the butler *i* + 1.

Voting for the butler candidate: Butler *j* sends requests to all commissioners for voting. After collecting and counting the ballot tickets, butler *j* generates a special block with election results and related records. Then butler *j* will send this block to all commissioners for validation.

Each block generates a random number that determines who will be the next voter, which ensures that butlers generate blocks in a random order. The random number generation algorithm is as follows:
Suppose butler receives signature from K commissioners, represented by

$$signature(i); \left(0 \le i \le K, \frac{Nc}{2} \le K \le Nc - 1\right) \quad (1)$$

The time it is received from the server is TimeStramp.
Voter authorization made by following equations,

$$R = \left(\sum_{i=0}^{K-1} signature\,(i) \right) \oplus Timestramp \qquad (2)$$

Voter validation can be done by following equation

$$VV = \big(Hash(R)\big) mod\, N_b \qquad (3)$$

Based on VV value voter validation made if this value above 0.51 then he is a valid voter otherwise proxy voter.

IV. Security Analysis of Consensus Algorithm

In this the analysis of E-voting using POW and POV consensus algorithms has been made. This simulation made by using NS-3 emulator and it is assumed that the number of commissioners Nc=500 and number of voters Nv=10lakhs.

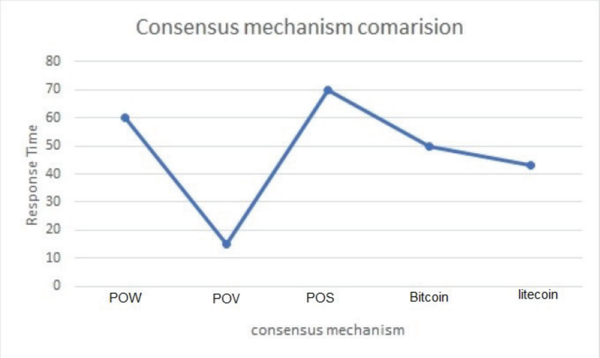

Figure 5. Comparison of different consensus protocols

Figure 5 Shows the comparison of different consensus algorithms. This analysis is made on block chain implementations and creating smart contacts using NS3. From above it is concluded that Proof of voting has fast response time for block creation as compared to other consensus mechanisms.

E-voting system using BCT is a distributed type network. Every ballot box in the network act as node and every node is connected to network. This distributed network does not allow any other malicious nodes. In this paper security analysis is made by byzantine failures. In POW the byzantine failure percentage is more comparing with POV. The statistical analysis will prove the result. Table 1 will give the total information about this.

TABLE I.
Comparison Statement of Pow VS POV

Consensus Mechanism	Byzantine failures	Smart contacts
Proof-Of-Work (POW)	5%	Very slow
Proof-Of-Voting (POV)	3.2%	Fast

V. Conclusions

In this paper, a unique blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy is introduced and also outlined the systems architecture, the design and a security analysis of the system.

References

[1] M. T. Isaai, F. Firoozi and M. R. Hemyari, "E-election in Digital Society," 2009 Third International Conference on Digital Society, Cancun, 2009, pp. 24-29.

[2] S. S. Dash, C. Shekhar, S. Kumar and R. K. Agrawal, "Leveraging ICT for election 2014 results dissemination," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 2170-2172.

[3] L. Sandberg, S. Jaradat and N. Dokoohaki, "The social media election agenda: Issue salience on Twitter during the European and Swedish 2014 elections," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, 2016, pp. 793-794.

[4] S. A. Adeshina and A. Ojo, "Design imperatives for e-voting as a sociotechnical system," 2014 11th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, 2014, pp. 1-4.

[5] G. Wang, Z. Shi, M. Nixon and S. Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 166-175.

[6] S. Homayoun, A. Dehghantanha, R. M. Parizi and K. R. Choo, "A Blockchain-based Framework for Detecting Malicious Mobile Applications in App Stores," 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 2019, pp. 1-4.

[7] H. L. Pham, T. H. Tran and Y. Nakashima, "A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract," 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.

[8] S. V., A. Sarkar, A. Paul and S. Mishra, "Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 1075-1079.

[9] S. Saini and J. Dhar, "An Eavesdropping Proof Secure Online Voting Model," 2008 International Conference on Computer Science and Software Engineering, Hubei, 2008, pp. 704-708.

[10] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao and C. Wang, "Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, 2018, pp. 636-644.

[11] N. Torii and M. Kitakami, "A Method for Stable Block Generation Time in Proof of Work," 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), Kyoto, Japan, 2019, pp. 53-531.

[12] Y. Shang, "Finite-Time Weighted Average Consensus and Generalized Consensus Over a Subset," in IEEE Access, vol. 4, pp. 2615-2620, 2016.

[13] S. Pahlajani, A. Kshirsagar and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," 2019 1st

International Conference on Innovations in Information and Communication Technology (ICIICT), CHENNAI, India, 2019, pp. 1-6.

[14] X. Liu and H. Ma, "Privacy Preserving Finite-time Consensus in Networks With Time-varying Topology," 2019 34rd Youth Academic Annual Conference of Chinese Association of Automation (YAC), Jinzhou, China, 2019, pp. 312-316.

[15] D. Kim, R. Ullah and B. Kim, "RSP Consensus Algorithm for Blockchain," 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 2019, pp. 1-4.

[16] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019.

[17] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 184-193.

[18] X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 261-265.

[19] L. Wan, D. Eyers and H. Zhang, "Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 194-201.

[20] N. Baranwal Somy et al., "Ownership Preserving AI Market Places Using Blockchain," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 156-165.