International Journal of Engineering Researches and Management Studies

A NOVEL VERIFIABLE RANDOM RANKING BASED SECURE BLOCKCHAIN CONSENSUS ALGORITHM FOR IOT-APPLICATIONS IN HEALTHCARE

Manish Pundlik, Kavita Choudhary
School of Computers, IPS Academy, Indore, M.P., India
manishpundlik71@gmail.com
School of Computers, IPS Academy, Indore, M.P., India

ABSTRACT

The use of IoT offerings improves human existence in lots of approaches. Protection towards cyber threats is an utmost important prospect of IoT gadgets operation. Malicious sports result in exclusive records leakage and incorrect performance of devices turns into critical. Therefore, development of powerful answers that can protect each IoT devices in healthcare facts and records exchange networks turns in to an actual venture. Aiming at some critical issues within the current consensus algorithms, this paper proposes the verifiable random ranking (VRR) based Secure Blockchain Consensus (SBC) mechanism to clear up the issues raised above. In comparison to standard algorithms, we reinvented methods to assess node reliability and robustness and manage lively nodes. Our experiments display that the VRR–SBC algorithm has lower consensus delay, higher throughput, improved safety, and lower verification charges. The simulation consequences show efficiency of the blockchain era for restrained devices and give the opportunity to evaluate applicability limits of the selected consensus algorithm.

KEYWORDS: IoT, Blockchain, Security, Consensus mechanism, Trust primarily based Ranking.

1. INTRODUCTION

With the development, continuous improvement and development of technology which include sensor generation, pc manage generation, embedded technology, and wi-fi network records verbal exchange, the Internet of Things (IoT) has shown remarkable improvement worldwide [1]. As IoT devices in healthcare are aid-limited in terms of processing, storage and community potential, it turns into a hard task to ensure the get admission to of IoT gadgets. Its timeliness, comfort, inclusiveness, scalability, integration, and interoperability make IoT an unheard-of prospect for in addition development [2]. However, security dangers regarding service provisioning and records sharing also increases. There are many present safety procedures, although these approaches are not suitable for IoT gadgets due to their restricted storage and constrained computation assets. In current years, with the emergence of blockchain, the concept of combining blockchain and IoT has won tremendous interest [3]–[5].

Blockchain technology has obtained more interest in current years [6]–[8], because of its inherent homes of immutability and decentralization. Blockchain era has superior swiftly in current years and is now widely used in an expansion of fields. Due to the attributes of Blockchain which include decentralization, immutability, auditability, transparency, and cryptographic security, it offers numerous blessings to unique domain names inclusive of cryptocurrency, financial sectors, non-public/public segments, coverage, healthcare, deliver chain control, IoT, and so forth [9]. The decentralization supplied by way of blockchain may be largely attributed to using consensus mechanism, which enables peer-to-peer trading in a disbursed way without the involvement of any third party. However, the technology is in its early stage and still, there may be a number worries which can be but to be addressed before its huge adoption [10].

Blockchain has been appeared as a promising era for IoT, since it gives significant answers for decentralized network which can cope with accept as true with and protection concerns, high renovation price hassle, and so forth [11]. Blockchain appears to be one of the excellent solutions for coping with massive heterogeneous gadgets at the same time as achieving superior statistics security and records trust, mainly in the subject of massive-scale IoT network [12]. The speedy evolution in blockchain technology, which trusted a decentralized, immutable and dispensed ledger system for transaction statistics auditing, affords a potential way to cope with the troubles in IoT [13]. The blockchain era offers possible answers for the identity authentication and protection protection of IoT gadgets. The threshold of deployment and management blockchain is exceedingly low [14]. Even if the clever gadgets have confined computing sources, blockchain may be deployed. Applying blockchain within the IoT makes the centralized community structure emerge as decentralized or multicentralized, which can significantly enhance the security of the machine [15].

Emerging research in IoT packages exploits blockchain technology to file transaction data, optimize contemporary machine performance, or construct subsequent-technology structures, that may offer additional protection, computerized transaction management, decentralized systems, offline-to-online data verification, and so forth [16] [17]. According to, the traits of IoT dispensed and open get entry to, the IoT architecture attempts to introduce blockchain era to remedy the safety hassle of IoT tool records, so that everyone gadgets can interact with the outside global underneath the control of the user [18]. The IoT is a use case which can take benefit of these particular Blockchain homes. IoT gadgets are normally implemented in sensitive domains including fitness, clever cities, and supply chains. Resilience and facts integrity are crucial for these domains, as disasters and malicious data tampering can be detrimental to the structures that depend upon those IoT gadgets [19]. Additionally, Blockchains are well perfect for decentralised networks and networks with high churn fees. A difficulty concerned with applying Blockchain era to the IoT is the dearth of computational assets. This manner that conventional consensus mechanisms like Proof of Work (PoW) are mistaken. By leveraging the capabilities of tamper-proof and decentralized consensus mechanism in blockchain, we have the chance to solve the safety issues in IoT structures [20].

To overcome the shortcomings of traditional consensus mechanism, a Trust primarily based verifiable random rating mechanism changed into proposed on this paper. The following contributions are made in this research.

- We recommend a unique believe based ranking set of rules for IoT-blockchain programs. The protocol utilizes trust facts and timestamp from IoT devices in healthcare to ensure the reliability of nodes and enhance blockchain security via a deposit penalty mechanism.
- Verifiable random ranking (VRR) mechanism in VRR–SBC ensures equity and randomness while electing nodes within the IoT blockchain device.
- We construct a blockchain prototype with the VRR–SBC protocol and carried out sizeable experiments with round 40 nodes (simulate server machines as IoT gadgets). The proposed VRR–SBC set of rules indicates existing algorithms like PBFT with better consensus performance, throughput, and lower communication overhead within the community.

2. RELATED WORK

Xu et al. [21] identified and given an in-depth review of cutting-edge blockchain networks, key matrix of designing consensus mechanism for IoT networks in phrases of throughput, scalability and protection. Meshcheryakov et al., [22] provided an important evaluation of the feasibility of the use of blockchain technology to defend restrained IoT devices in healthcare facts, justifies the selection of Practical Byzantine Fault Tolerance (PBFT) consensus algorithm for implementation on such gadgets, and simulated the principle allotted ledger scenarios using PBFT. Queralta et al. [23] reviewed existing consensus protocols and scalability techniques in each properly-established and subsequent-era blockchain architectures. Yuan et al. [24] proposed the Efficient Byzantine Trust-based Consensus (EBRC) mechanism to solve the terrible node reliability, low transaction according to second (TPS) rates, and scalability problems. Zhang et al., [25] proposed a light-weight statistics consensus algorithm for the Industrial Internet of Things (IIoT) based totally on blockchain technology to make sure at ease records transmission within the IIoT for smart city applications.

Rim Ben Fekih and Mariam Lahami [26] have found various examples of how the blockchain age is being employed in the country of art, such as for exchanging digital clinical data, remote patient monitoring, drug distribution chains, and so on. The objective of Xiaomin Du et al. [27] was to investigate the application of blockchain technology in smart healthcare, establish a hierarchical theoretical framework of smart healthcare, reveal the impact of blockchain on smart healthcare, and ultimately construct a development utility system of smart healthcare based on the blockchain and the stakeholder concept. Erik Westphal and Hermann Seitz [28] investigated current research on particular blockchain implementations in healthcare that go beyond the state of idea research or theoretical implementation ideas. Deepa Elangovan et al. [29] employed a systematic review strategy to uncover literature related to the adoption of blockchain technology in quality healthcare. Partha Pratim Ray et al. [30] analysed blockchain systems for their suitability in IoT-based e-healthcare and explored the well-known consensus methods employed in blockchain in the context of e-health. Blockchain technology was employed to assist the elderly with appropriate timing, consistent tracking, managing a database of their clinical facts and vital signs, and keeping track of any irregularities by Aishwarya Gowda et al. [31]. Meyliana et al. [32] carried out qualitative research on the use of blockchain generation, which has traits including immutability, unchangeability, and peer-to peer, to be able to minimise the opportunity for counterfeit capsules. G.S. Gunanidhi and R. Krishnaveni [33] proposed an "Enhanced Proof of Work (E-PoW)" consensus blockchain consortium approach for IoT-based completely healthcare tracking devices to improve data safety and privacy, thereby lowering bandwidth and improving efficiency. Abubakar et al. [34] identified four fundamental additives, as well as their design issues and barriers, that must be considered when developing a blockchain-primarily based structure for the IoT, and they mentioned four standard blockchain-primarily based completely IoT architecture patterns.

3. PROPOSED VRR–SBC MECHANISM

Blockchain, as an open, cozy and allotted transaction ledger technology, can flexibly adapt to complicated and changing community environments. The failure of some nodes does no longer have an effect on the solid operation of the machine. However, it's far vital to pick out the failure nodes. For that reason, in this paper a VRR–SBC mechanism is proposed. The ordinary process framework of the VRR–SBC mechanism relevant to the IoT blockchain is shown in

Figure 1.

Trust Evaluation
Trust Growth Rate Evaluation
VRR Random Ranking
VRR–SBC consensus protocol
Integrity verification

Figure 1: Overall process framework of the VRR–SBC mechanism

(i) Trust evaluation of nodes

For each node in the system, an actual number with a trust value between (0,1] is defined. The trust value, which represents the credibility of the corresponding node, is set to 0.5 for newly added nodes. Furthermore, in order to become a consensus node, the node must pay a deposit, which affects the calculation of the trust value. The trust evaluation process is explained in the following algorithm 1.

```
Algorithm 1
Input: Node Set
    $X$ ,
Output: Trust value of each node
    $T_x$
for all
    ( ) $\forall T_i \in T_x$ do
    calculate ������,��
        �� ��,��
    calculate ����$^{��}$(�������������) = [(∑ ����
        ��=0 ��$^{����}$)(��$^{����}$)$^{-1}$]
end
```

The satisfaction value , is calculated from the feedback reply from each node using table1.

Table 1: Satisfaction Value Calculation

Satisfaction Values	Condition
1.0	Very satisfied
0.5	Satisfied
0.3	Neutral
0.1	Not satisfied
0	Not satisfied

Above table1 speaks to the states of agreeable qualities. To manage potential changes of the hub, conduct after some time, we utilize an overlooking component which helps in doling take away load to more established feedback reactions.

(ii) Trust growth rate evaluation

The calculation of trust value and trust growth rate is carried out around the behavior record table. Before the end of each epoch, the current consensus master node initiates a request to update the trust value and trust growth rate. The specific implementation is shown in Algorithm 2.

```
Algorithm 2

Input: Node Set
                    $X$ ,Old record table $RT_{old}$
Output: New record table
                                $RT_{new}$
while
        $RT_{old}$do
Read (
        $RT_{old}$);
                                $^{t}R_{i\,x}R_{i\,t}O\ t$ =;
                    ( ) [( / ) -1]*100 $^{1/\ -1}$
Calculate
                                , .
Update (
          $RT_{old}$);
end
$RT_{new}$= $RT_{old}$;
VRR–SBC(
              $RT_{new}$);
Return
         $RT_{new}$;
```

After receiving the request, the consensus node calculates the new trust value of the entire network according to the local behavior record buffer pool. It then uses the VRR–SBC consensus protocol proposed in this paper to reach a consensus on the trust value. After the consensus is completed, the master node updates the node’s trust, whose trust value and trust growth rate have changed in this round into the behavior record table and broadcast it on the entire network. The system then enters the next round of the consensus ranking stage.

(iii) VRR random ranking mechanism

Nodes with different trust values and trust growth rates have different ranking permissions. The VRR mechanism was explained in algorithm 3.

```
Algorithm 3
Input: New record table
        $RT_{new}$, Number of consensus node set
                $Y$
                $CN$, candidate consensus node
Output: consensus node set
        $CN_S$, consensus node
set
    $CCN_S$
```

```
While
RTnewdo
Read
RTnew
Sort (
RTnew,R)
end
S P (hash(t -1)); =
RNG
L VRR(S (S)); = k
Pr oof VRRPr oof(S (S)); = k
if L ≤ϑthen 256 / 2
Broadcast–connect message(
(P ,Proof ,Sign); k
else end
if current.validator==consensus node and messge.type==connect and node I
ranks  in the top 85% in the trust and trust rate collections then
VRR (msg.P , S,msg.Pr oof) verify k;
VRRverifythen
if
Add CN i
( , );
S
ifcount CN R
( , )
S
CN top nodes
85% ;
=
CCN bottom nodes
=
15% ;
S
else end
else end
else end
CNS, CN , CCNS
return
```

(iv) VRR–SBC consensus protocol

consensus process is shown in Figure 2.

This paper proposes VRR–SBC to solve the consensus algorithm's security issues. The Client R3 P R1 R2
1
request
prepare
prepare
commit
Reply

Figure 2: consensus process

VRR–SBC consensus protocol was explained in algorithm 4.

Algorithm 4

```
                                                    $CN$, candidate consensus
Input: consensus node set
                                  $CN_S$, consensus node
node set
            $CCN_S$, consensus Master node
                                          $CN_M$
                                      $CN$ .
Output: Reliable consensus node

         $CN$and
for all
                    $CN_M$do
Broadcast$<< C_{req} ,t,d,m(d),c >,Sig_c >$
verify if the node is $CN$
   $CN$is valid,
if
verify if transaction is valid,
Broadcast $<< \Pr epare,h,v,t,d,m(d) >,Sig_M >>$
else end
else end
verify the Master node
                              $CN_M$
Broadcast $<< commit,v,t,m(d),sn,valid /invalid >,Sig_i >$ $CN$receives identical
     acknowledgment messages, a consensus is
all
reached, and the client’s request will be executed,
Now the client will reply
                                        $<< reply,c,t,m(d),n,valid /invalid >,Sig_i >$
end
          $CN$
return
```

(v) Integrity verification

The hash of the critical data of each device has stored into blockchain in the process of registration. During the execution of the task, the IoT nodes periodically send an integrity verification request for the critical data to the neighboring node. If the verification fails, it indicates that a key configuration file has been tampered with and a warning will be triggered. In addition to the firmware and configuration files of the IoT devices in healthcare, the data collected and the log files generated by the devices during the execution of the task can also be saved into blockchain after hashing the data for data protection and security audit.

4. EXPERIMENTAL RESULTS AND ANALYSIS

To verify the applicability of the VRR–SBC consensus algorithm, we designed different experiment schemes with following specifications.

• Server machines: Intel Core i7 2.2 GHz CPU with 16 GB DRAM and 256 GB SSD • OS: Ubuntu 16.04

- Simulation networks: Sawtooth PBFT 1.0 with EBRC
- The initial consensus committee IoT devices: 4
- Maximum number of IoT devices : 40.

The performance analysis is carried out in terms of transaction delay, throughput, communication time, ranking fairness, and communication complexity.

4.1 Transaction delay

We tested the transaction delay of VRR–SBC, PBFT and EBRC algorithm under each of the following nodes: 4, 7, 10, 13, 19, 25, 31, and 40, where represents the number of nodes in the blockchain; 15 blocks with different numbers of transactions are tested. Every block was tested 15 times. And then, the latency of the VRR–SBC, EBRC algorithm and the PBFT algorithm was compared by taking the average latency of each block.

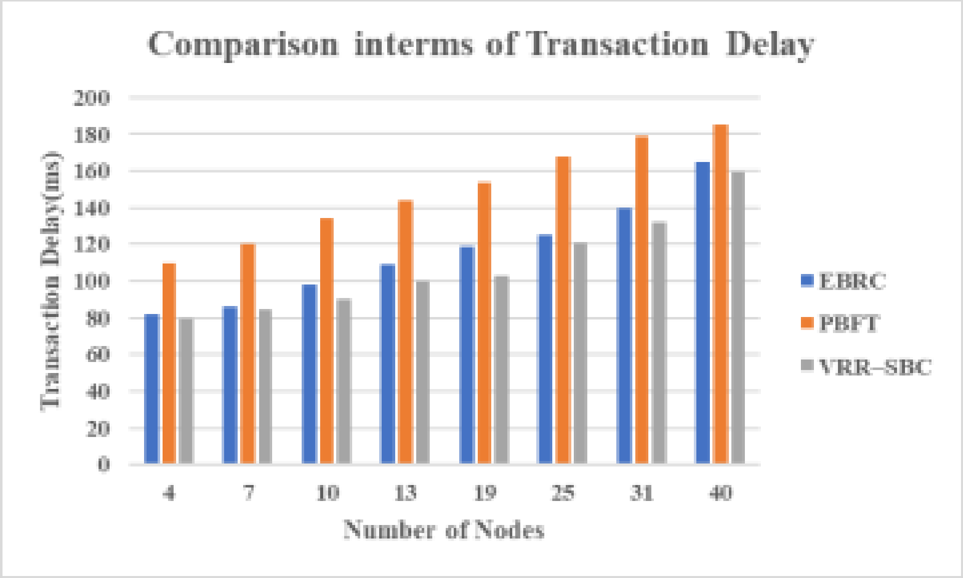

Figure 3: Comparison interms of transaction delay

As shown in Figure 3, the transaction delay of the proposed VRR–SBC algorithm is lower than EBRC and PBFT algorithm. From figure 3, it can also be seen that blocks with different numbers of transactions affect latency.

4.2 Throughput

The client initiated 100 transactions, and we observed the transaction throughput performance of VRR–SBC, PBFT and EBRC algorithms under the different numbers of nodes: 4, 7, 10, 13, 19, 25, 31, and 40. The result is shown in Figure 4.

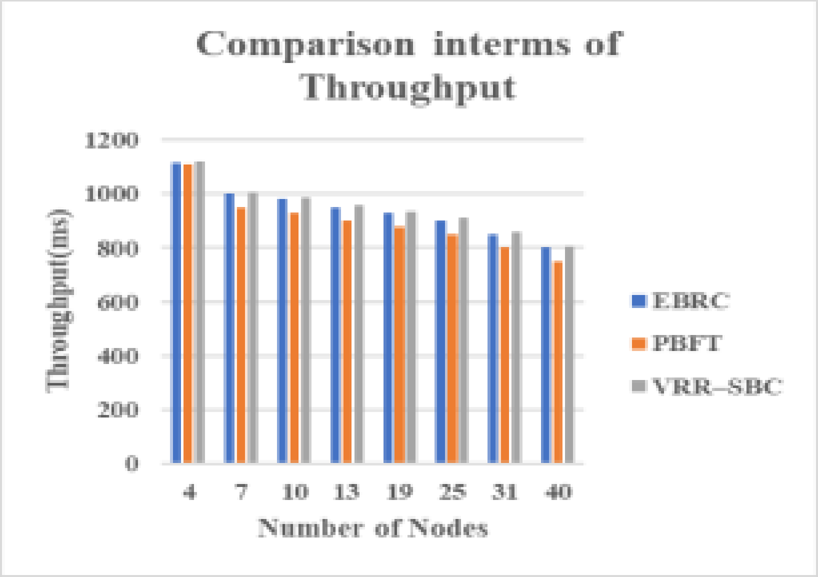

Figure 4: Comparison interms of Throughput

As shown in figure 4, the throughput of the two algorithms decreases as the nodes increase. However, the throughput of the VRR–SBC is slightly higher than the EBRC algorithm and significantly higher than PBFT algorithm.

4.3 Communication time

The time consumed during the transaction VRR–SBC, PBFT and EBRC algorithms are compared in figure 5.

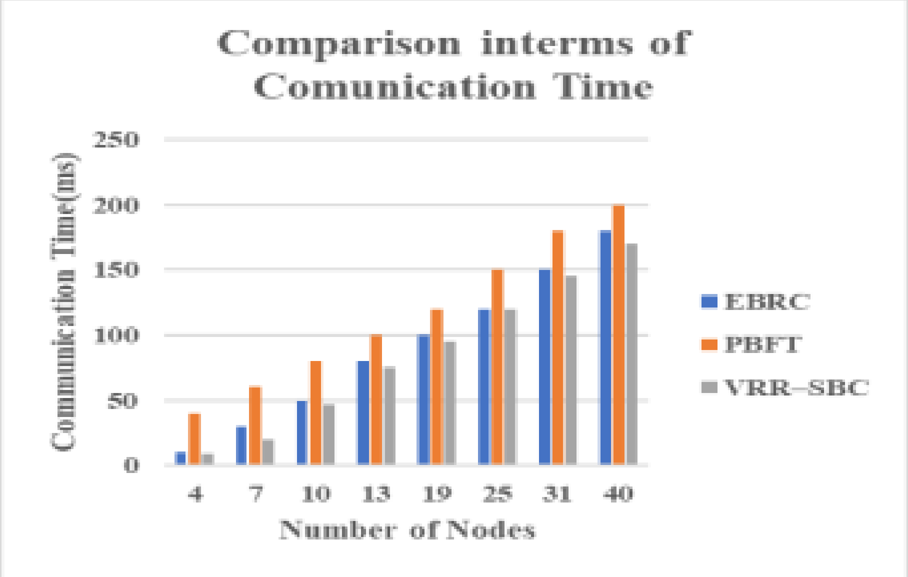

Figure 5: Comparison interms of communication time

It can be seen from Figure 5, it is seen that the communication time increases with the increase in number of nodes. However, the communication time of VRR–SBC algorithm is relatively low compared to PBFT and EBRC algorithms.

4.4 Communication complexity

We compare the communication complexity of the proposed VRR–SBC algorithm with the existing algorithms such as PBFT, DBFT, EPBFT, Trust-PBFT, T-PBFT, Tu, and EBRC in figure 6.

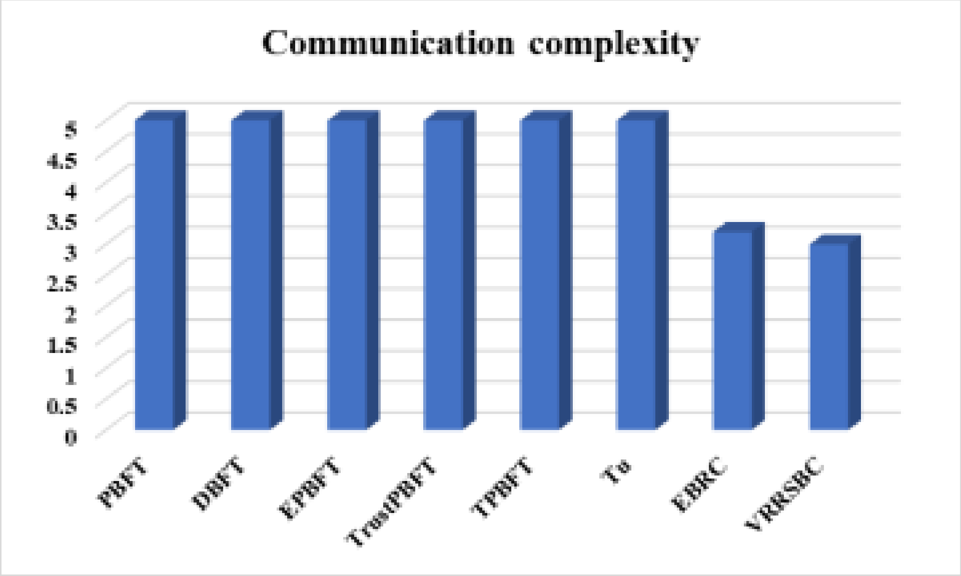

Figure 6: Comparison interms of communication complexity

From figure 6, it is visible that the communication complexity of the proposed algorithm is comparatively lower than the existing algorithms.

4.5 Ranking fairness of Proposed Ranking Mechanism

To test the fairness of the ranking process, we create 20 nodes and set all the nodes' trusts to a default value of 0.5. We ran 12000 experiments to give all the nodes enough time to evaluate. We tested the number of times the node was ranked as a consensus node (including candidate consensus nodes), as shown in Figure 7. The number of times that a node is ranked is an even distribution, ranges from 48 to 51, proving that the ranking of nodes is fair.

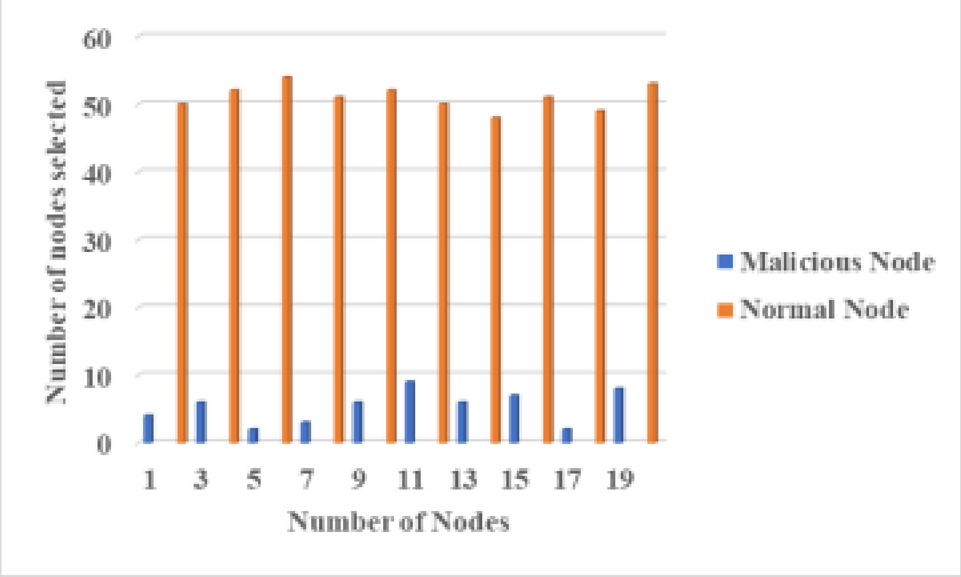

Figure 7: Comparison interms of ranking fairness

It is also observed that as the error rate increases, the number of times a node is ranked as a consensus node decreases fourfold compared to a regular node, demonstrating that if the node does not follow the protocol, the decreased credibility value will impact the ranking's chances of success. It also takes a long time for nodes to recover from disruptive actions.

5. CONCLUSION

In this paper, we have proposed a novel ranking mechanism based on the trust values of the nodes was proposed to design a secure blockchain consensus mechanism for healthcare applications. The proposed VRR–SBC achieves high consensus efficiency, low network overhead, and high scalability by trust-based node ranking. By integrating the VRR random ranking algorithm, we randomly selected the high trust node to join the consensus. Finally, extensive experiments were conducted to indicate the superior performance of VRR–SBC over the traditional PBFT consensus mechanism, indicating that our proposed algorithm can provide an effective solution for the construction of the secure blockchain.

REFERENCES

1. Wu, Yue, Liangtu Song, Lei Liu, Jincheng Li, Xuefei Li, and Linli Zhou. "Consensus mechanism of IoT based on blockchain technology." Shock and Vibration 2020 (2020). [2] Lin, Weijun, Xinghong Huang, Hui Fang, Victoria Wang, Yining Hua, Jingjie Wang, Haining Yin, Dewei Yi, and Laihung Yau. "Blockchain technology in current
2. agricultural systems: from techniques to applications." IEEE Access 8 (2020): 143920- 143937.
3. [3] Tsang, Yung Po, King Lun Choy, Chun Ho Wu, George To Sum Ho, and Hoi Yan Lam. "Blockchain-driven IoT for food traceability with an integrated consensus mechanism." IEEE access 7 (2019): 129000-129017.
4. [4] Huang, Junqin, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism." IEEE Transactions on Industrial Informatics 15, no. 6 (2019): 3680-3689.
5. [5] Cao, Bin, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou, and Mugen Peng. "When Internet of Things meets blockchain: Challenges in distributed consensus." IEEE Network 33, no. 6 (2019): 133-139.
6. [6] He, Qingqiang, Nan Guan, Mingsong Lv, and Wang Yi. "On the consensus mechanisms of blockchain/dlt for internet of things." In 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), pp. 1-10. IEEE, 2018.
7. [7] Lao, Laphou, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang. "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling." ACM Computing Surveys (CSUR) 53, no. 1 (2020): 1-32.
8. [8] Si, Haiping, Changxia Sun, Yanling Li, Hongbo Qiao, and Lei Shi. "IoT information sharing security mechanism based on blockchain technology." Future Generation Computer Systems 101 (2019): 1028-1040.
9. [9] Qiao, Liang, Shuping Dang, Basem Shihada, Mohamed-Slim Alouini, Robert Nowak, and Zhihan Lv. "Can blockchain link the future?." Digital Communications and Networks (2021).
10. [10] Da Xu, Li, Yang Lu, and Ling Li. "Embedding blockchain technology into IoT for security: A survey." IEEE Internet of Things Journal 8, no. 13 (2021): 10452-10473. [11] Wang, Eric Ke, RuiPei Sun, Chien-Ming Chen, Zuodong Liang, Saru Kumari, and Muhammad Khurram Khan. "Proof of X-repute blockchain consensus protocol for IoT systems." Computers & Security 95 (2020): 101871.
11. [12] Auhl, Zachary, Naveen Chilamkurti, Rabei Alhadad, and Will Heyne. "A Comparative Study of Consensus Mechanisms in Blockchain for IoT Networks." Electronics 11, no. 17 (2022): 2694.
12. [13] Sri, PSG Aruna, and D. Lalitha Bhaskari. "Blockchain technology for secure medical data sharing using consensus mechanism." Materials Today: Proceedings (2020).
13. [14] Shrimali, Bela, and Hiren B. Patel. "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities." Journal of King Saud University Computer and Information Sciences (2021).
14. [15] Liu, Tao, Yi Yuan, and Zhongyang Yu. "The service architecture of Internet of things terminal connection based on blockchain technology." The Journal of Supercomputing 77, no. 11 (2021): 12690-12710.
15. [16] Mo, Bing, Kuiren Su, Songjie Wei, Cai Liu, and Jianping Guo. "A solution for internet of things based on blockchain technology." In 2018 IEEE international conference on service operations and logistics, and informatics (SOLI), pp. 112-117. IEEE, 2018.
16. [17] Tian, Zongqing, Biwei Yan, Qiang Guo, Jianyun Huang, and Qingyu Du. "Feasibility of identity authentication for IoT based on Blockchain." Procedia Computer Science 174 (2020): 328-332.
17. [18] Alghamdi, Turki Ali, Ishtiaq Ali, Nadeem Javaid, and Muhammad Shafiq. "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain." IEEE Access 8 (2019): 1048-1061.
18. [19] Xu, Xiaojun, Lu Hou, Yankai Li, and Yunxin Geng. "Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application." In 2021 7th International Conference on Computer and Communications (ICCC), pp. 1520-1525. IEEE, 2021.
19. [20] Rehman, Mubariz, Nadeem Javaid, Muhammad Awais, Muhammad Imran, and Nidal Naseer. "Cloud based secure service providing for IoTs using blockchain." In 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1-7. IEEE, 2019.
20. [21] Xu, Ronghua, Yu Chen, and Erik Blasch. "Microchain: A Light Hierarchical Consensus Protocol for IoT Systems." In Blockchain Applications in IoT Ecosystem, pp. 129-149. Springer, Cham, 2021.
21. [22] Meshcheryakov, Yaroslav, Anna Melman, Oleg Evsutin, Vladimir Morozov, and Yevgeni Koucheryavy. "On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices." IEEE

Access 9 (2021): 80559-80570.

22. [23] Queralta, Jorge Peña, and Tomi Westerlund. "Blockchain for mobile edge computing: Consensus mechanisms and scalability." In Mobile Edge Computing, pp. 333-357. Springer, Cham, 2021.
23. [24] Yuan, Xu, Fang Luo, Muhammad Zeeshan Haider, Zhikui Chen, and Yucheng Li. "Efficient Byzantine consensus mechanism based on trust in IoT blockchain." Wireless Communications and Mobile Computing 2021 (2021).
24. [25] Zhang, Wenbo, Zonglin Wu, Guangjie Han, Yongxin Feng, and Lei Shu. "LDC: A lightweight dada consensus algorithm based on the blockchain for the industrial Internet of Things for smart city applications." Future Generation Computer Systems 108 (2020): 574-582.
25. [26] Ben Fekih, R., & Lahami, M. (2020). Application of blockchain technology in healthcare: A comprehensive study. In the Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18 (pp. 268-276). Springer International Publishing.
26. [27] Du, Xiaomin, Beibei Chen, Ming Ma, and Yanjiao Zhang. "Research on the application of blockchain in smart healthcare: constructing a hierarchical framework." Journal of Healthcare Engineering 2021 (2021).
27. [28] Westphal, Erik, and Hermann Seitz. "Digital and decentralized management of patient data in healthcare using blockchain implementations." Frontiers in Blockchain 4 (2021): 732112.
28. [29] 1. The Use of Blockchain Technology in the Health Care Sector: Systematic Review (Elangovan D, Long CS, Bakrin FS, Tan CS, Goh KW, Yeoh SF, Loy MJ, Hussain Z, Lee KS, Idris AC, Ming LC The Use of Blockchain Technology in the Health Care Sector: Systematic Review JMIR Med Inform 2022;10(1):e17278).
29. [30] 3. Deepak Sharma, Sudhir Kumar Sharma, Chapter 10 - The use of blockchain technology in IoT-based healthcare: A concise guide, Editor(s): Bharat Bhushan, Sudhir Kumar Sharma, Muzafer Saračević, Azedine Boulmakoul, In Cognitive Data Science in Sustainable Computing,Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems, Academic Press, 2023, Pages 183-198.
30. [31] 4. A. G. A G, H. -K. Su and W. -K. Kuo, "Blockchain-based Healthcare System for Elderly Care," 2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), Tainan, Taiwan, 2022, pp. 144-147, doi: 10.1109/ECBIOS54627.2022.9945042.
31. [32] 6. Meyliana, Surjandy, E. Fernando, C. Cassandra and Marjuki, "Medicine Information Record Based on Blockchain Technology," 2021 2nd International Conference on Innovative and Creative Information Technology (ICITech), Salatiga, Indonesia, 2021, pp. 169-173, doi: 10.1109/ICITech50181.2021.9590133.
32. [33] 7. G. S. Gunanidhi and R. Krishnaveni, "Improved Security Blockchain for IoT based Healthcare monitoring system," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1244- 1247, doi: 10.1109/ICAIS53314.2022.9742777.
33. [34] 8. Abubakar, M., Ali, H., Ghaleb, B., Wadhaj, I., Buchanan, W.J. (2023). An Overview of Blockchain-Based IoT Architectures and Designs. In: Al-Sharafi, M.A., Al-Emran, M., Al-Kabi, M.N., Shaalan, K. (eds) Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems. ICETIS 2022. Lecture Notes in Networks and Systems, vol 584. Springer, Cham. https://doi.org/10.1007/978- 3-031-25274-7_52