

Comparison of PoW and PoA Consensus Mechanisms in Blockchain Technology Using WSN

Dr. Satpal Singh¹, Dr. Arwinder Singh²

¹University College Chunni Kalan, Punjabi University, Patiala

²University College Ghanaur, Punjabi University, Patiala

Abstract

Blockchain technology has become a viable way to improve Wireless Sensor Networks' (WSNs') security, transparency, and dependability. Nonetheless, the performance, scalability, and energy efficiency of these systems are greatly impacted by the consensus mechanism selection. In the context of blockchain-integrated WSNs, this paper compares two popular consensus algorithms: Proof of Work (PoW) and Proof of Authority (PoA). Key performance metrics such energy usage, processing overhead, latency, scalability, and security are the main emphasis of the analysis. The findings show that PoW is appropriate for WSNs because after the attack, the blockchain remains valid and maintains its integrity, ensuring that the stored data is accurate and consistent. PoA, on the other hand, is inappropriate for WSN contexts, it compromises the integrity of the blockchain, making it less trustworthy and susceptible to manipulation.

Introduction:

Blockchain is utilized to make our system secure because of its property of immutability. Moreover, it can handle transactions with enhanced security as it undergoes to a complex hashing algorithm SHA256. Blockchain is distributed ledger that can continuously grow and store a large amount of data. Mining is the process to append a new block onto the chain and this task is completed by the miners. Many nodes in the network compete with each other in order to mine a block and get reward. We already go through a lot many consensus algorithms i.e. PoW, PoA, PoC etc. that help us deduce a miner.

Blockchain-based system can be improved by considering the following:

1. Scalability: As more users join the system, it becomes challenging to handle the increasing number of transactions. To improve scalability, the system can be optimized to process transactions more efficiently or use a sharding mechanism to divide the network into smaller sub-networks.
2. Security: Security is a critical aspect of any blockchain system. The system can be improved by using advanced cryptographic algorithms and implementing more robust consensus mechanisms to prevent malicious actors from compromising the network.
3. Usability: Blockchain systems can be challenging to use, particularly for non-technical users. Improving the usability of the system by simplifying the user interface and making it more intuitive can encourage broader adoption.
4. Interoperability: Different blockchain networks often have difficulty communicating with each other. To improve interoperability, the system can be designed to be compatible with other blockchain networks, allowing for the seamless transfer of assets and data between different networks.

5. Sustainability: Blockchain systems require a significant amount of energy to operate. To improve sustainability, the system can be designed to consume less energy by using more energy-efficient algorithms or by leveraging renewable energy sources.

Wireless Sensor network has improved the quality of life by providing easy way to interact with remote devices without any physical connection. Along with certain advantages, WSN is prone to various hacking attacks and viruses, Attackers can attack any node in the network and change the routing data according to their need. In sybil attack, a node declares itself with several false identities and try to interlink with other nodes to modify the routing data. A person attempts to create too many false nodes in order to gain the control of whole network. Sybil attack has been detected in WSN using machine learning by Mandala *et al.* Dhamodharan *et al.* detect and prevent the sybil attacks in WSN using combined CAM-PVM (compare and match-position verification method) with MAP (message authentication and passing). Sybil attack means to dissimulate its identification to all other nodes which results in data loss and becomes harmful for the system. Attackers can ruin the entire network by creating a lot of fake identities which results in leaving out the true nodes to transmit and receive data.

In our proposed work, we identify and prevent sybil attack using Blockchain technology. There are numerous consensus mechanisms in Blockchain to deduce the miner like PoW (Proof of Work), PoS (Proof of Stake), PoA (Proof of Authority) etc. In blockchain, if the attacker manages to take control of 51% of nodes, it can alter the transactions. Actually, consensus mechanisms help the users to transmit data by increasing the difficulty level to keep it away from the attackers. We have implemented both PoA and PoW to tackle with sybil attack. In Proof of Work, a miner needs to solve the cryptographic problem in order to get the rights to add a new block in the blockchain. In Proof of Authority, a few numbers of pre-defined nodes get the authority to act as validators and append new block to the network.

Literature Review:

Sung-Jung Hsiao *et al.* proposed a technique to improve the security of data in blockchain based WSN. They use microcontrollers to interconnect various sensor nodes and security is being enhanced by utilizing blockchain technology. In this, the proposed system acts as private cloud data centre that visualises the data uploaded by the sensors to create charts and tables. Integration of blockchain technology with wireless sensor network is thoroughly explained in this paper. To simplify the blockchain security, they shift the encryption method from asymmetric to symmetric.

Nguyen *et al.* discussed various benefits and shortcoming of blockchain technology in WSN. By using sensors, it becomes easier to collect data from our surroundings thus it makes life more comfortable. The major benefits of using BC in WSN are security, immutability, reliability and shared system. However, it also has some drawbacks like storage issue, scalability, power consumption, lack of skills and legal issues. Mubarakali presented a novel efficient approach for authentication using blockchain technology to secure the routing data in Wireless Sensor Networks. Base stations, sink nodes and normal nodes are being formulated for simulation purposes. A hybrid model is made by integrating the blockchain technology with WSN in which user authentication and verification is done through BC.

Godawatte *et al.* secured the information accountability and integrity in healthcare using BC. Sensors devices are prone to attacks as they are low capability devices. Blockchain provides WSN security features along with data breach prevention methods. Majority of the nodes in WSN are low powered devices so they may or may not be suitable for deployment in BC. In healthcare, extremely sensitive data is passed

through the sensors, altering in data by malicious node can be lethal for the patient's life. Future cloud computing and fog computing will use BC to protect WSN transmission.

Ramasamy *et al.* introduced a survey on BC based WSN for malicious node detection. It detects the malicious node in two parts, firstly, the BC based WSN architecture for malicious node detection and secondly, smart contract aspect in malicious node detection. Then this survey explains the data management, security management, information integrity and node longevity in wireless sensor network. In the end, paper provides the information of data sharing, storage requirements, malicious node detection and data security.

Nguyen *et al.* presented the framework of deploying BC in WSN. Attackers can attack the network to get the desired information from the network. The main purpose of this paper is to reduce the attack from the hackers and improve efficiency by detecting malicious nodes. Blockchain has decentralized consensus mechanisms that helps in preventing the data tampering. The most modern security and data storage technology available nowadays is blockchain. Moreover, BC is managed by all the nodes of network and authentication message is broadcasted to each node in the network.

Paulraj *et al.* proposed the security mechanism in blockchain based WSN by using authentication and cluster head selection. Cluster heads receive the data from the sensor nodes and process it according to the requirement. DDR- LEACHE can be substituted with CHs if the distance of BS, residual energy and degree are considered. Many computational resources and power were needed to implement PoW so it was being replaced by PoA. In the end, MITM and Sybil were used to calculate the results and check the system's resilience.

Awan *et al.* proposed a blockchain based encryption and trust evaluation model in which aggregator nodes and sensor nodes are stored. Authentication of AN is checked by public blockchain whereas SN's authentication is performed by private blockchain. SNs are more prone to attacks because these are of low power, less transmission range and limited computational capabilities. PDR is high when there is large number of trusted SNs but PDR is low when most of the SNs die due to low energy and only few SNs participate. Rivest-Shamir-Adleman (RSA) is used for encryption and decryption of data for secure transmission.

Shahbazi *et al.* collected the human psychological and physical data (Blood pressure, ECG, temperature, sugar level etc.) from the patients that demands secure, optimal and efficient routing techniques. A blockchain based Adaptive Thermal/ Energy-Aware Routing (ATEAR) protocol is used for data transmission. Temperature rise, throughput and energy consumption are used to evaluate the performance of ATEAR whereas resource utilization, latency and transaction throughput are used to investigate BC performance.

Qu and Zheng *et al.* submitted an efficient routing protocol in Wireless body area network in order to perform reliable data transmission. They take many parameters into consideration like residual energy, transmission efficiency, available bandwidth and number of hops to the sink node. A maximum benefit function to select the next hop node by normalizing the node parameters and select the node with largest value as next hop node. The proposed work is compared with priority-based energy efficient routing algorithm (PERA) which shows the improvement in reliability of data transmission.

Methodology:

Blockchain enhances the security and reliability of Wireless Sensor Network, since it works without involving any third party. Blockchain is decentralized and distributed, hence it proves to be a most efficient

approach for authentication in WSN. Wireless Networks use a wide variety of sensor devices in order to transmit data from one place to another so they are much prone to the attacks. Blockchain network is protected by SHA256 cryptography encryption and works according to the consensus mechanism. Each block of the blockchain contains hash of the previous block, timestamp and data sensed by the devices. It is extremely difficult for the hackers to tamper the data of blockchain. In our proposed work, first of all, we collect the routing data by using Q-tables in MATLAB. After that, we upload this .mat file i.e. routing data to the blockchain. We stick to the following procedure to record the routing data.

1. Firstly, all the parameters are initialized such as network size, number of nodes, number of rounds, cluster heads and energy constants.
2. All the nodes in wireless sensor network are represented by structure array S. Random coordinates (xd, yd) are being assigned to every node. E is the initial energy of each node. Sink node acts a central point to receive data from all the cluster heads.
3. Learning parameters alpha (learning rate) and gamma (discount factor) are being set and the Q-table is initialized with zeros.
4. Now, the code runs for rmax rounds which will work as follows:
 - a. Cluster heads are selected according to some probability calculations and energy levels of the nodes.
 - b. Consumption of energy for each node is derived on the basis of distance to its respective cluster head or the sink node.
 - c. Q-learning action selection is done for every node having energy by using epsilon-greedy exploration and Q value is updated as per the reward obtained by state-action pair.
 - d. Other statistics like number of cluster heads, packets transmitted to sink and cluster heads and network energy are updated for each round.

In the end, the learned Q-table is saved as a .mat file for further usage in blockchain.

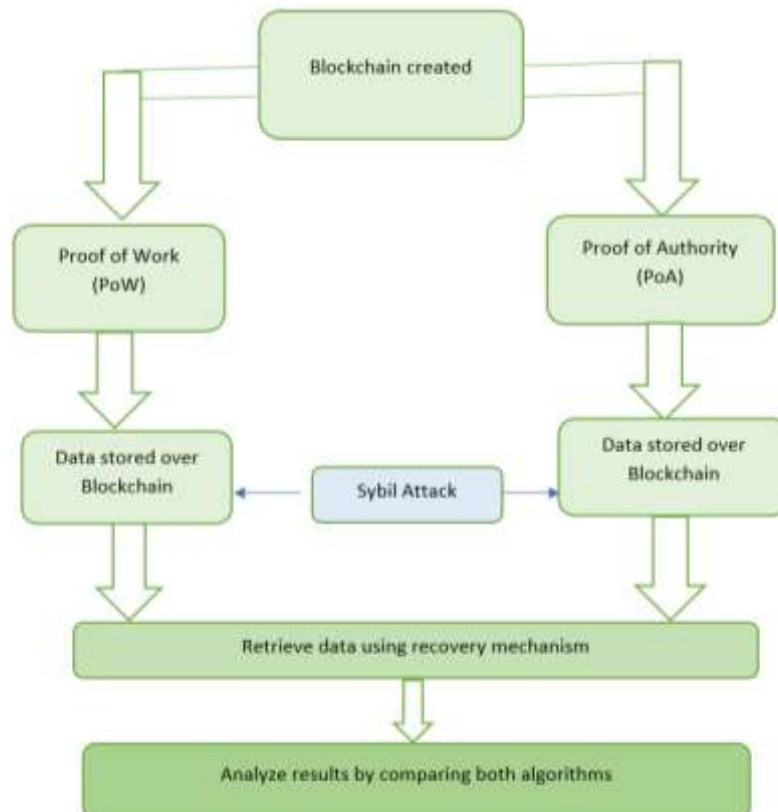


Fig. 2: - Sybil Attack over Blockchain network

In the next step, we upload this .mat file to the blockchain in order to analyse its security by using two consensus algorithms PoW (Proof of Work) and PoA (Proof of Authority). We have tried to attack the nodes of blockchain to check its integrity and justify blockchain security by reverting the last three blocks. This sybil attack is performed, detected and prevented by using PoW and PoA algorithms. Firstly, blockchain is being created and PoA is applied to store the data over this blockchain, then we perform sybil attack and retrieve the data using recovery mechanism. After that, same procedure is done using PoW algorithm. We verify the size of retrieved data with the uploaded one, if both the files are of equal size then we consider that there is no data loss in our uploaded file and we have prevented the sybil attack.

Results:

All things considered, PoW guarantees greater security and data dependability while PoA provides superior performance and energy efficiency. Therefore, PoW is still preferred for security-critical situations that demand high integrity and trust, whereas PoA may be more appropriate for resource-constrained WSN applications where speed and energy efficiency are objectives.

Table 1- : Comparison of key security parameters for both PoW and PoA algorithms

Security Parameter	PoW	PoA
Time taken to add block	31,145,040 nanoseconds	46,521 nanoseconds
Sybil Attack Detection	15,696 nanoseconds	3,765 nanoseconds
Blockchain Validity	True	False
Blockchain Integrity	Maintained	Breached
Blockchain Resilience	High	Low
Recovery Time	1,774 nanoseconds	N/A

- Time taken to add a block: PoW takes longer to add a block due to the computational effort required for proof-of-work, while PoA is faster as it relies on authority validation.
- Sybil Attack Detection: PoW takes longer to detect a potential Sybil attack compared to PoA.
- Blockchain Validity: PoW maintains the validity of the blockchain after a Sybil attack, while PoA fails to maintain validity.
- Blockchain Integrity: PoW maintains integrity even after a Sybil attack, while PoA is breached.
- Blockchain Resilience: PoW demonstrates high resilience against a Sybil attack, while PoA shows low resilience.
- Recovery Time: PoW has a recovery time of 1,774 nanoseconds to revert the attack and recover the blockchain, while PoA does not have a recovery mechanism.

Based on the analysis, PoW appears to provide stronger security guarantees in terms of maintaining the validity, integrity, and resilience of the blockchain in the face of a Sybil attack. It also provides a recovery mechanism to revert the attack. However, PoW requires more computational resources and time compared to PoA, which can be a factor to consider depending on the specific use case and requirements.

In the tabular security analysis, the term "Blockchain Resilience" refers to the ability of the blockchain to withstand a Sybil attack and recover from it. It indicates the level of effectiveness in maintaining the correctness and consistency of the blockchain in the presence of an attack.

In the case of PoW (Proof of Work), the blockchain demonstrates high resilience against a Sybil attack. This means that even after the attack, the blockchain remains valid and maintains its integrity, ensuring that the stored data is accurate and consistent.

On the other hand, in the case of PoA (Proof of Authority), the blockchain shows low resilience against a Sybil attack. This implies that the attack compromises the integrity of the blockchain, making it less trustworthy and susceptible to manipulation.

Overall, resilience is a crucial aspect of blockchain security as it reflects the system's ability to recover from attacks and maintain its trustworthiness. Higher resilience indicates a stronger security posture, ensuring that the blockchain remains reliable and secure even in the face of adversarial actions.

Conclusion and Future Scope:

The performance and security behavior of PoW and PoA consensus techniques in blockchain-enabled Wireless Sensor Networks (WSNs) differ significantly, according to a comparative investigation. PoW takes significantly longer to add a block (31,145,040 ns) than PoA (46,521 ns), suggesting that PoA validates transactions more quickly. PoW has greater robustness, with correct blockchain validity (True), sustained integrity, and excellent resistance against attacks, including faster Sybil attack detection (15,696 ns) and recovery time (1,774 ns). Security metrics, however, reveal a different trend. PoA, on the other hand, shows signs of weakness when authority nodes are corrupted, including decreased resilience, integrity breaches, and invalid blockchain states.

All things considered, PoW guarantees greater security and data dependability while PoA provides superior performance and energy efficiency. Therefore, PoW is still preferred for security-critical situations that demand high integrity and trust, whereas PoA may be more appropriate for resource-constrained WSN applications where speed and energy efficiency are objectives.

As we have completed first two objectives of our work, our next goal is to train the model using reinforcement learning according to the dataset retrieved from blockchain. We will train the model by implementing Q-learning algorithm in Python. Then we will save the trained routing table in .mat format for making optimal routing decisions in network. In the end, we will run simulations and generating plots in order to differentiate routing protocols in WSN. Results will be analysed by comparing various parameters of four routing protocols (LEACH, LEACH-Centralized, TSI-LEACH and Q-LEACH).

References:

1. Mandala Mounica *et al* (2021). Detecting Sybil Attack In Wireless Sensor Networks Using Machine Learning Algorithms *IOP Conf. Ser.: Mater. Sci. Eng.* 1042 012029 DOI 10.1088/1757-899X/1042/1/012029
2. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method. *The Scientific World Journal*, 2015, 841267. doi:10.1155/2015/841267
3. Arshad, A., Mohd Hanapi, Z., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. *PeerJ. Computer science*, 7, e673. <https://doi.org/10.7717/peerj-cs.673>
4. Zhukabayeva T. K; Mardenov E. M; Abdildaeva A.A (2020). *Sybil Attack Detection in Wireless Sensor Networks*. doi:10.1109/AICT50176.2020.9368790.

5. Sung-Jung Hsiao, W.-T. S. (2021). Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission. *Computers, Materials & Continua*, 68(2), 1899–1918. doi:10.32604/cmc.2021.015762.
6. Nguyen, Van-Cuong & Nguyen, Minh & B, Trang & Tran, Thang & Duy, Nguyen. (2021). Blockchain Technology in Wireless Sensor Network: Benefits and Challenges. 1-5.
7. Mubarakali, A. (2022). An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. *Wireless Pers Commun* 127, 255–269 <https://doi.org/10.1007/s11277-021-08212-w>.
8. Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., Loy, M. J., Hussain, Z., Lee, K. S., Idris, A. C., & Ming, L. C. (2022). The Use of Blockchain Technology in the Health Care Sector: Systematic Review. *JMIR medical informatics*, 10(1), e17278. <https://doi.org/10.2196/17278>.
9. Godawatte, K., Branch, P., & But, J. (2022). Use of blockchain in health sensor networks to secure information integrity and accountability. *Procedia Computer Science*, 210, 124–132. doi:10.1016/j.procs.2022.10.128.
10. Ramasamy, L. K., Khan K. P., F., Imoize, A. L., Ogbemor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey. *IEEE Access*, 9, 128765–128785. doi:10.1109/ACCESS.2021.3111923.
11. Nguyen, M., Nguyen, C., & Tran, H. T. (2022). A Framework of Deploying Blockchain in Wireless Sensor Networks. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 9(32), e3. <https://doi.org/10.4108/eetinis.v9i32.1125>.
12. Paulraj D., Jayasudha, L. R, T., Ishwarya M, N., Daniya T. and Daniel S, F. (2023). "Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, pp. 1-5, doi: 10.1109/ICICACS57338.2023.10099593.
13. Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. *Sensors (Basel, Switzerland)*, 22(2), 411. <https://doi.org/10.3390/s22020411>.
14. Shahbazi, Z., & Byun, Y. C. (2020). Towards a Secure Thermal-Energy Aware Routing Protocol in Wireless Body Area Network Based on Blockchain Technology. *Sensors (Basel, Switzerland)*, 20(12), 3604. <https://doi.org/10.3390/s20123604>.
15. Qu, Y., Zheng, G., Wu, H., Ji, B., & Ma, H. (2019). An Energy-Efficient Routing Protocol for Reliable Data Transmission in Wireless Body Area Networks. *Sensors (Basel, Switzerland)*, 19(19), 4238. <https://doi.org/10.3390/s19194238>.
16. Zhang, G., Zhang, Y., & Chen, Z. (2013). Using trust to secure geographic and energy aware routing against multiple attacks. *PloS one*, 8(10), e77488. <https://doi.org/10.1371/journal.pone.0077488>.
17. Bangotra, D. K., Singh, Y., Kumar, N., Kumar Singh, P., & Ojeniyi, A. (2022). Energy-Efficient and Secure Opportunistic Routing Protocol for WSN: Performance Analysis with Nature-Inspired Algorithms and Its Application in Biomedical Applications. *BioMed research international*, 2022, 1976694. <https://doi.org/10.1155/2022/1976694>.
18. Kumar, M., Mukherjee, P., Verma, S., Kavita, Kaur, M., Singh, S., Kobielnik, M., Woźniak, M., Shafi, J., & Ijaz, M. F. (2022). BBNSF: Blockchain-Based Novel Secure Framework Using RP^2 -RSA and

- ASR-ANN Technique for IoT Enabled Healthcare Systems. *Sensors (Basel, Switzerland)*, 22(23), 9448. <https://doi.org/10.3390/s22239448>.
19. Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. *Sensors (Basel, Switzerland)*, 11(2), 1345–1360. <https://doi.org/10.3390/s110201345>
20. Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors (Basel, Switzerland)*, 19(22), 4954. <https://doi.org/10.3390/s19224954>.