**RESPONSE TO REVIEWERS’ COMMENTS RECEIVED FOR OUR SUBMISSION “***A Novel Blockchain Structure for Wireless Sensor Networks Based on IOTA Tangle*” (**Manuscript ID:** electronics-1758170)

**ROUND 2**

The authors thank the anonymous reviewers for the in-depth scrutiny, and valuable feedback and suggestions, which have improved the quality of the paper. In the following, we provide responses to the reviewers’ comments. The sentences highlighted in blue font are the new additions in the revised manuscript. These changes have been incorporated into our revised manuscript.

**REVIEWER 1**

**Reviewer 1, Comment 1:***-The standardization of this class of protocols is already very advanced and it is not clear the contribution of the work in relation to the state of the art.*

**Authors’ Response:**

Thank you for this comment. New paragraph is added in Section 1, Introduction, line 54~60.

Although the standardization of protocols is advanced, the main focus of our paper is different. What we propose is a network topology for data transmission designed for WSNs, which will validate and store the sensed data submitted by WSN nodes in the gateway in an application scenario. It enables WSNs to process information securely and efficiently under restricted sensor nodes. Current protocol standardization does not address this aspect, so we believe the proposal provides a new solution for the application of blockchain and IOTA in WSNs.

**REVIEWER 2**

*-The paper “A Novel Blockchain Structure for Wireless Sensor Networks Based on IOTA Tangle” presents an interesting and timely topic. The current version of the manuscript presents improvements but still needs work before being ready for publication.*

**Reviewer 2, Comment 1:***-The proposal and difference with IOTA are now clear. However, some key concepts in the introduction and problem definition must be addressed.*

*-First, since the authors are stressing the difference between WSN and IoT on resource constraints, they should introduce and discuss current approaches addressing blockchain for constrained sensors. For instance, they should mention current research that has addressed Blockchain for IoT (10.1109/COMST.2018.2886932), and highlight the challenges that IoTA solves. Similarly, they should at least reference current research tackling constrained sensors and blockchain (10.1109/ICCWorkshops49005.2020.9145328, 10.1109/ICBC48266.2020.9169404, ) . All these works can help set the reference of their proposal in the context of current research.*

**Authors’ Response:**

Thank you for these suggestions. New paragraphs are added in Section 2.5, related work, line 163~190. The articles mentioned are cited.

Ali, Vecchio et al [34] have conducted an excellent survey on IoT and its challenges pertaining to network security, user privacy, data management, and standardization. Blockchain features can address several of these challenges. For example, the distributed nature of Blockchain can help in maintaining data backups and thus provide data integrity after an attack. The advantages of adaptability can help IoT devices to adapt to different application platforms and environments. The anonymity and tamper-evident characteristics can counter some network attacks that target modifying data. Blockchain does not require a trusted third party to process transactions but uses smart contracts that enable the counterparties to trust each other. Blockchain also has advantages over centralized data storage in terms of cost. Researchers have introduced many blockchain-based IoT solutions which show that blockchain has significant advantages for addressing IoT challenges in terms of trust, network security, identity management, and data monetization.

Pincheira and Vecchio [35] propose an architecture to integrate blockchain into resource-constrained IoT sensors. The integration of blockchain on sensing devices can make the collected data trustworthy by using the decentralized and tamper-proof features of Blockchain. The researchers analyzed and experimented with the proposed architecture based on real application scenarios of public utility management systems in terms of cost, memory footprint, processing time and power consumption. They concluded that the architecture is suitable for constrained IoT devices and that the application cost for utility management could be less than 1 USD per device per month.

In the area of agricultural traceability, Pincheira et al [36] analyzed the impact of applying Blockchain to the IoT on its sensors. The researchers tested six IoT boards on the Ethereum and Hyperledger Sawtooth platforms in terms of disk usage, memory usage, processing time, and power consumption. The results showed that blockchain applications for IoT outperformed Sawtooth on Ethereum. Pincheira et al [37] proposed a technology framework for water management that is a combination of IoT and Blockchain. The experimental results show that the interaction between IoT and Blockchain causes 6% additional energy consumption in this application.

**Reviewer 2, Comment 2:***-Another concern that needs to be addressed more clearly is the security and decentralization of IOTA (or not blockchain-based Distributed Ledger Technology) compared to Blockchain-based approaches.*

*-In Table 1 . The* *security comparison between Blockchain and IoTA, only with “YES” is quite weak. Security and how it is achieved is a key difference between the two DLT approaches. The authors should address this point in the table and in the previous paragraphs 2.3 and 2.4. Additionally, they should highlight the trade-offs in terms of security that IOTA makes in comparison with traditional blockchain, so it can achieve the benefits it presents. See http://dx.doi.org/10.2139/ssrn.3144241 for reference.*

**Authors’ Response:**

Thank you for this suggestion. New paragraph is added in Section 2.3. Blockchain Technology, line 107~111. The article mentioned is cited.

Blockchains use decentralized consensus mechanisms to ensure data security, such as PoW (Proof of Work) [26]. PoW is the process of mining, and the network nodes used to calculate the hash values are the miners. Miners obtain different hash values by changing nonce in the block header and when the hash value reaches the target, the new block will be broadcasted to other nodes to verify the hash value and attach it to blockchains [23].

New sentence is added in Section 2.4. IOTA Tangle, line 128~131.

COO is the consensus mechanism in IOTA, which is emitted every two minutes to randomly select two new transactions for approval, and the transactions approved by the COO are considered fully trusted [28].

Table 1 updated, removed security comparison. New sentences added to line 139~144.

|  |  |  |
| --- | --- | --- |
| Table 1. Comparison of Some Features of Traditional Blockchain and IOTA Tangle [5] [28] [30] [31] [32] [33]. | | |
| Feature | Blockchain | IOTA Tangle |
| Decentralized | Yes | Yes |
| Distributed | Yes | Yes |
| Tamper-proof | Yes | Yes |
| Scalability | Low | High |
| Latency | High | Low |
| Mining Process | Yes | No |
| Transaction Fee | Yes | No |
| Processing Time | Long | Short |
| Efficiency (Transactions per second) | 3-4 | 500-800 |
| Suitable Transaction Type | General Transactions | Small Transactions |
| Transaction Validation | Miner | Self-validation |
| Throughput | Low | High |
| Resource Requirements | High | Low |
| Consensus (Proof of Work) | SHA256-Hash | Check Tangle Tips |
| Openness | Public Ledger | Public Ledger |

Traditional blockchains use mining to verify transactions, whereas in the IOTA Tangle, transactions are confirmed through tips checking and COO verification. The mining process has great requirements on the computing power of the device, and IoT devices that generate a large number of small transactions may not be able to mine, so the security mechanism of IOTA is more suitable for IoT.

**Reviewer 2, Comment 3:***-Finally, I understand that there are no similar works to compare. However, the authors should at least be able to find and discuss related works that, for instance, propose other methods to reduce the load of DLT for making them suitable for IoT, even with constrained devices. For instance, there is a survey of Blockchain for IoT where these topics are addressed (doi 10.1109/COMST.2018.2886932). Furthermore, there is also work related to blockchain in very constrained IoT devices (dois 10.1109/ICCWorkshops49005.2020.9145328 and https://doi.org/10.1007/978-3-030-86162-9\_21). Presenting these types of works will make their proposal stronger, as they show why the topic is important and why their solution is innovative.*

**Authors’ Response:**

Thank you for the suggestion. As outlined in the Response for Reviewer 2, Comment 1, new paragraphs are added in Section 2.5, related work, line 163~190. The articles mentioned are cited.

**Reviewer 2, Comment 4:***-Regarding the use of English, some paragraphs need a bit of rewriting for easier reading and connectivity. For instance, 2.2 Internet of things has too many short sentences that read like a bullet list rather than a continuous paragraph.*

**Authors’ Response:**

Thank you for the comment. We have reorganized Section 2.2 and fixed grammar issues in other sections.

Internet of Things (IoT) is a network infrastructure consisting of uniquely identifiable interoperable connected objects that communicate and exchange data with other devices and systems using technologies such as Radio Frequency Identification (RFID) technology and WSNs [14]. Several communication, network, sensing, and information processing devices are interconnected to form an IoT system [15]. IoT devices can communicate with each other and interact with users through the network by equipping various devices with components such as microcontrollers and communication transceivers [16]. IoT connects the physical and virtual worlds to sense, communicate, interact, and exchange data [17]. IoT can be applied to many fields such as smart homes, wearable devices, smart cities, healthcare, and industrial applications [18], [19], [20], [21].

**REVIEWER 3**

**Reviewer 3, Comment 1:***-The authors need to proof read the paper for grammatical and structural errors.*

**Authors’ Response:**

Thanks very much for the comment. We have thoroughly proofread the paper and corrected grammatical and structural errors.

**Reference**

[5] Bhandary, M.; Parmar, M.; Ambawade, D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 827–832. https://doi.org/10.1109/ICCES48766.2020.9137858.

[14] Hassan, W.H.; et al. Current research on Internet of Things (IoT) security: A survey. Computer networks 2019, 148, 283–294.

[15] Da Xu, L.; He,W.; Li, S. Internet of things in industries: A survey. IEEE Transactions on industrial informatics 2014, 10, 2233–2243.

[16] Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. IEEE Internet of Things Journal 2014, 1, 22–32. https://doi.org/10.1109/JIOT.2014.2306328.

[17] Porkodi, R.; Bhuvaneswari, V. The internet of things (IOT) applications and communication enabling technology standards: An overview. In Proceedings of the 2014 International conference on intelligent computing applications. IEEE, 2014, pp. 324–329.

[18] Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. IEEE Internet of Things Journal 2018, 5, 3758–3773. https://doi.org/10.1109/JIOT.2018.2844296.

[19] Adamu, A.A.; Wang, D.; Salau, A.O.; Ajayi, O. An integrated IoT system pathway for smart cities. International Journal on Emerging Technologies 2020, 11, 1–9.

[20] Salau, A.O.; Chettri, L.; Bhutia, T.K.; Lepcha, M. IoT based smart digital electric meter for home appliances. In Proceedings of the 2020 International Conference on Decision Aid Sciences and Application (DASA). IEEE, 2020, pp. 708–713.

[21] Rana, A.K.; Salau, A.O.; Sharma, S.; Tayal, S.; Gupta, S. Internet of Things: Energy, Industry, and Healthcare; CRC Press, 2021.

[23] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85.

[26] Li, X.; Jiang, P.; Chen, T.; Luo, X.;Wen, Q. A survey on the security of blockchain systems. Future Generation Computer Systems 2020, 107, 841–853.

[28] Silvano,W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future generation computer systems 2020, 112, 307–319.

[30] Hao, Y.; Li, Y.; Dong, X.; Fang, L.; Chen, P. Performance Analysis of Consensus Algorithm in Private Blockchain. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 280–285. https://doi.org/10.1109/IVS.2018.8500557.

[31] Zhou, Z.; Li, R.; Cao, Y.; Zheng, L.; Xiao, H. Dynamic Performance Evaluation of Blockchain Technologies. IEEE Access 2020, 8, 217762–217772. https://doi.org/10.1109/ACCESS.2020.3040875.

[32] Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access 2020, 8, 126927–126950. https://doi.org/10.1109/ACCESS.2020.3006078.

[33] Schueffel, P. Alternative distributed ledger technologies Blockchain vs. Tangle vs. Hashgraph-A high-level overview and comparison. Tangle vs. Hashgraph-A High-Level Overview and Comparison (December 15, 2017) 2017.

[34] Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 2019, 21, 1676–1717. https://doi.org/10.1109/COMST.2018.2886932.

[35] Pincheira, M.; Vecchio, M. Towards Trusted Data on Decentralized IoT Applications: Integrating Blockchain in Constrained Devices. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1–6. <https://doi.org/10.1109/ICCWorkshops49005.2020.9145328>.

[36] Pincheira, M.; Vecchio, M.; Giaffreda, R. Benchmarking Constrained IoT Devices in Blockchain-Based Agri-Food Traceability Applications. In Proceedings of the International Congress on Blockchain and Applications. Springer, 2021, pp. 212–221.

[37] Pincheira, M.; Vecchio, M.; Giaffreda, R.; Kanhere, S.S. Exploiting constrained IoT devices in a trustless blockchain-based water management system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–7. https://doi.org/10.1109/ICBC48266.2020.9169404.