Blockchain-IIOT: Enhancing Data Integrity and Trust in industrial IOT with Proof of Authority Algorithm (BIIOT)

Technical Report · May 2024

DOI: 10.13140/RG.2.2.15214.22081

2 authors, including:

Barnabas Ukwuani
University of South Dakota
1 PUBLICATION **0** CITATIONS

SEE PROFILE

Blockchain-IIOT: Enhancing Data Integrity and Trust in industrial IOT with Proof of Authority Algorithm (BIIOT)

Barnabas Ukwuani
Computer Science Department
University of South Dakota
Vermillion, SD
Barnabas.ukwuani@coyotes.usd.edu

Okechukwu Ndubuisi
Computer Science Department
University of South Dakota
Vermillion, SD
okechukwu.ndubuisi@coyotes.usd.edu

Saadudeen Saadu
Computer Science Department
University of South Dakota
Vermillion, SD
saadudeen.saadu@coyotes.usd.edu

***Abstract*— The Industrial Internet of Things (IIoT) revolutionizes industrial operations, yet challenges in data integrity, security, and energy efficiency persist. Traditional centralized systems are vulnerable, necessitating innovative solutions. This paper proposes leveraging blockchain with Proof of Authority (PoA) consensus to address these challenges. Through a review of related work, the proposed PoA architecture, methodology, and empirical evaluation, this research demonstrates PoA's effectiveness in enhancing security, trust, data integrity, and energy efficiency in IIoT environments. The findings highlight the importance of blockchain in industrial settings, offering practical insights for secure and efficient IIoT implementations.**

I. Introduction

With the exponential growth of Industrial Internet of Things (IIoT) systems in industrial settings, characterized by the interconnection of numerous devices, sensors, and machinery, these systems optimize operations, enhance efficiency, and reduce downtime, crucial for maintaining operational reliability, regulatory compliance, and business continuity. However, challenges related to data integrity, security, energy efficiency, and trustworthiness hinder the full penetration of IIoT in the industrial sector. Ensuring the integrity and trustworthiness of data generated and exchanged within IIoT ecosystems is critical. The abundance of data in the industrial space also presents vulnerabilities, including data tampering, unauthorized access, and malicious attacks. Traditional centralized data management systems are susceptible to single points of failure and may not provide adequate security and resilience against threats, exacerbated by the heterogeneity of IIoT devices and systems. This lack of transparency and single points of failure pose significant challenges to data integrity and trust, especially in mission-critical industrial applications.

In response, innovative approaches leveraging emerging technologies like blockchain using the Proof of Authority (PoA) consensus algorithm are necessary to address these challenges and establish a secure and reliable foundation for data exchange and collaboration within IIoT ecosystems. In this paper, we propose a PoA-based consensus mechanism to address security, trust, data integrity, and energy efficiency concerns. PoA combines the security capabilities of PoW with improved transaction confirmation times. The paper is organized as follows: Section II reviews related work, Section III presents the proposed PoA architecture, Section IV outlines the methodology, Section V discusses results, and Section VI concludes with future directions.

II. Review of Related Works

Blockchain technology holds significant promise for revolutionizing industrial IoT (IIoT) ecosystems by enhancing security, efficiency, and trust in data management and exchange. Previous research and industry initiatives have explored various approaches to addressing the issue and many of them have varied from solutions over traditional centralised data management systems on Web 2.0 to distributed systems such as Blockchain on Web 3.0.

Two prominent consensus mechanisms, Proof of Work (PoW) and Proof of Stake (PoS), have been extensively studied in the context of IIoT applications. This review synthesizes insights from relevant literature to examine the implications of PoW and PoS for IIoT.

A. Proof of Work

PoW is the original consensus algorithm introduced by Bitcoin, where participants, known as miners, compete to solve complex mathematical puzzles to validate transactions and add blocks to the blockchain [1]. While PoW offers robust security against attacks, its energy-intensive nature and scalability limitations pose challenges, particularly in industrial IoT applications.

Li, Zhang, and Chen (2018) explore the application of blockchain technology in supply chain management and highlight the potential of PoW to enhance transparency and traceability in supply chain operations[2]. However, they also acknowledge the energy consumption issues associated with PoW, which may hinder its widespread adoption in industrial settings.

Dorri, Kanhere, and Jurdak (2017) focus on optimizing blockchain for IoT applications and discuss methods to improve scalability and efficiency[4]. They propose techniques to mitigate the energy consumption of PoW consensus in IoT environments, such as off-chain validation and consensus partitioning, to make it more suitable for resource-constrained devices.

B. Proof of Stake

PoS is an alternative consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold or stake in the network. PoS offers potential advantages over PoW, including reduced energy consumption and increased scalability, making it an attractive option for industrial IoT applications.

Kshetri (2017) investigates the potential synergies between blockchain and IoT and highlights PoS as a promising solution for enhancing security and privacy in IoT ecosystems [5]. The study discusses how PoS can address the energy consumption issues associated with PoW while

providing robust security and data integrity in industrial IoT deployments.

Wang et al. (2020) conduct a comprehensive survey on the application of blockchain in industrial automation systems and explore the role of PoS in improving efficiency and scalability [7]. They discuss various use cases where PoS consensus can facilitate secure and transparent data exchange among IoT devices, sensors, and industrial equipment, leading to more resilient and efficient industrial processes.

C. *Proof of Authority*

While PoW offers robust security, its energy consumption and scalability limitations may hinder its widespread adoption in industrial settings. PoS, on the other hand, offers potential advantages in terms of reduced energy consumption and increased scalability, making it a promising solution for enhancing security and efficiency in industrial IoT applications. Our approach for this experiment involves designing and developing a blockchain-IoT solution using the proof-of-authority consensus algorithm tailored to the specific requirements and challenges of Industrial IIoT environments. This will be compared to other consensus algorithms such as PoS and PoW. Our solution will also be integrable with existing IIoT infrastructure, including sensors, devices, and data management systems, to ensure seamless interoperability and minimal disruption to ongoing operations.

III. Proof of Authority Algorithm

Proof of Authority (PoA) is a consensus algorithm used in blockchain networks to achieve agreement on the validity of transactions and the ordering of blocks. Unlike Proof of Work (PoW) and Proof of Stake (PoS), where participants compete to validate transactions or create new blocks based on computational power or staked tokens, PoA relies on a set of trusted authorities to validate transactions and create new blocks.

In PoA, a predefined set of authority nodes is responsible for verifying transactions and adding blocks to the blockchain. These authority nodes are typically selected based on their reputation, identity, or stake in the network. Once a transaction is submitted, it is validated by one or more authority nodes, and upon consensus, the transaction is added to the blockchain.

IV. Methodology

Our research methodology follows a systematic approach to implementing a decentralized data management system and evaluating its performance based on three blockchain consensus algorithms: Proof of Authority (PoA), Proof of Stake (PoS), and Proof of Work (PoW). The methodology consists of several key steps, outlined below.

A. *Setup of Geth Nodes*

- Each consensus algorithm is implemented separately by setting up Geth nodes configured to utilize the designated algorithm.
- For PoA, the primary consensus algorithm, Geth nodes are configured accordingly to establish the network.

B. *Simulation of Consensus Algorithm*

- Each consensus algorithm is simulated with individual components to emulate real-world scenarios
- For PoA:
  - Worker nodes and Authority nodes are simulated to replicate the PoA consensus mechanism.
  - Smart contracts for data entry are created to facilitate transactions within the network.
- For PoS:
  - Nodes with varied stakes are simulated to reflect the PoS consensus model.
  - Smart contracts for data entry are generated to enable data transactions.
- For PoW:
  - Worker nodes are simulated to emulate the computational mining process inherent in the PoW consensus algorithm.
  - Smart contracts are established for data entry and transactions.

C. *Performance Evaluation Metrics.*

- Metrics such as energy efficiency, security, decentralization, scalability, and speed are employed to assess the performance of each consensus algorithm
- Performance metrics are recorded and rated based on observations and analysis of the simulated scenarios.

D. *Data Collection and Analysis.*

- Results from the simulations are systematically recorded, capturing relevant data and observations.
- The performance of each consensus algorithm is analyzed based on the predefined metrics.
- Comparative analysis is conducted to identify strengths, weaknesses, and trade-offs associated with each algorithm..

E. *Data Collection and Analysis.*

- Findings from the performance evaluation are synthesized and interpreted to draw conclusions regarding the effectiveness and suitability of each consensus algorithm.
- Insights gained from the evaluation process are used to inform recommendations for the selection and implementation of consensus algorithms in decentralized data management systems.

By following this research methodology, we aim to provide valuable insights into the performance characteristics of different blockchain consensus algorithms, thereby facilitating informed decision-making in the design and deployment of decentralized data management systems in various domains.

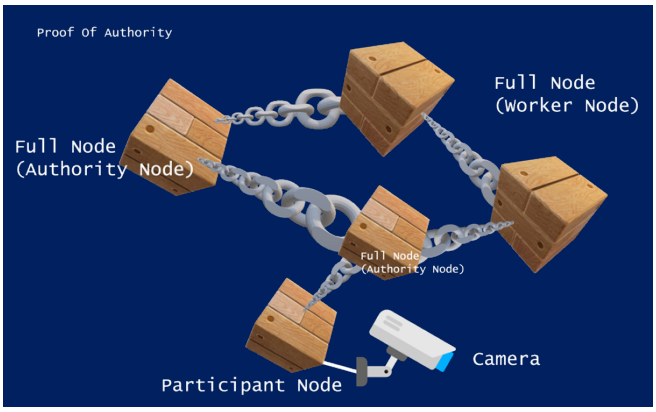

Fig. 1. Illustration of Proof of Authority

V. Result and Discussion

The comparison of consensus mechanisms—Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA)—reveals distinct performance characteristics across various factors, including energy efficiency, security, decentralization, scalability, and speed. The following discussion examines the implications of these findings and their relevance to decentralized data management systems.

The results observed were scaled on 5.

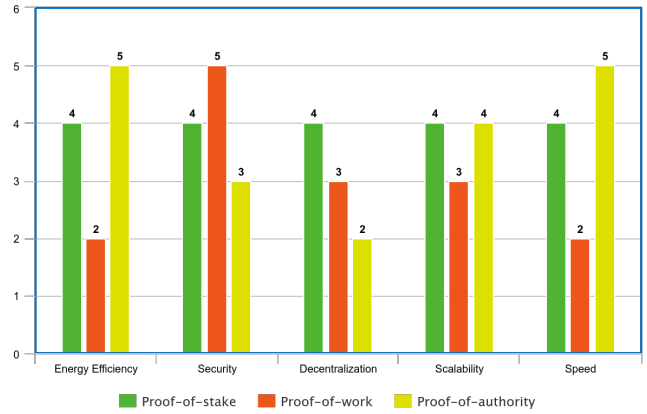

Fig. 2. Comparison of PoA, PoS, PoW

A. *Energy Efficieny:*

- PoW demonstrates the lowest energy efficiency among the three consensus mechanisms, scoring a mere 2. This result aligns with the resource-intensive nature of PoW, which relies on computational power for mining activities.
- PoS exhibits slightly better energy efficiency, scoring 4, as it mitigates the energy-intensive mining process by allowing nodes to validate transactions based on their stake in the network.
- PoA emerges as the most energy-efficient consensus mechanism, scoring 5, due to its reliance on a predetermined set of authority nodes for transaction validation, thus minimizing energy consumption associated with mining activities.

B. *Security:*

- PoW earns the highest score of 5 for security, reflecting its robustness against attacks due to the computational effort required to alter the blockchain.
- PoS follows closely with a score of 4, benefiting from the economic disincentives for malicious behavior imposed by the staking mechanism.
- PoA, while still secure, receives a slightly lower score of 3, as its security model relies on the trustworthiness of a designated set of authority nodes, which could potentially introduce centralization risks if compromised.

C. *Decentralization:*

- PoW and PoS both achieve moderate scores for decentralization, with PoW scoring 3 and PoS scoring 4. While PoW offers decentralized mining, it may suffer from the concentration of mining power among a few participants.
- PoS enhances decentralization by enabling broader participation in network validation, albeit with some degree of centralization based on stake distribution.
- PoA exhibits the lowest decentralization score of 2, reflecting its reliance on a predefined set of authority nodes, which could introduce centralization risks if these nodes collude or act maliciously, however, it does not have a single point of entry like centralized databases.

D. *Scalability:*

- PoW and PoA both score 3 for scalability, indicating moderate scalability potential. While PoW suffers from throughput limitations and scalability challenges due to the sequential nature of mining, PoA's scalability is constrained by the predetermined set of authority nodes.
- PoS stands out with a score of 4 for scalability, benefiting from its ability to achieve consensus through stakeholder participation without the resource-intensive mining process, thus enabling higher transaction throughput and network scalability.

E. Speed:

- PoW ranks the lowest in terms of speed, with a score of 2, reflecting its inherent latency in block generation and confirmation.
- PoS and PoA both exhibit higher speed, with PoS scoring 4 and PoA scoring 5. PoS benefits from its efficient consensus mechanism based on stakeholder validation, while PoA's reliance on a trusted set of authority nodes facilitates rapid transaction confirmation.

Discussion and implication:

- The choice of consensus mechanism plays a crucial role in determining the performance and characteristics of a decentralized data management system.
- While PoW offers robust security, it suffers from energy inefficiency and scalability limitations.
- PoS and PoA provide alternatives that prioritize energy efficiency, scalability, and speed, albeit with trade-offs in decentralization and security.
- The most suitable consensus mechanism based on demands in IoT is PoA as it prioritizes factors such as energy efficiency, speed and, scalability. It also performs averagely well on security and decentralization although not as good in comparison to others, these are trade-offs for energy consumption and speed.

In addition, this comparative analysis underscores the importance of considering multiple factors when evaluating consensus mechanisms for decentralized data management systems. By understanding the strengths and weaknesses of each mechanism, informed decisions can be made in the design and implementation of resilient and efficient blockchain-based solutions tailored for IoT in the industrial sector.

VI. Conclusion

In evaluating Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA) consensus mechanisms, each demonstrates distinct advantages and trade-offs.

While PoW offers unparalleled security, its energy inefficiency and scalability limitations are notable drawbacks. PoS improves on energy efficiency and scalability but introduces potential centralization risks.

In contrast, PoA emerges as a compelling choice, especially for industrial IoT (IIoT) applications, due to its energy efficiency, scalability, and speed. By designating trusted authority nodes, PoA eliminates energy-intensive mining while maintaining high security and reliability. Although PoA may sacrifice some decentralization, its suitability for private or consortium based IIoT deployments where trust is established makes it a promising option.

Ultimately, the choice of consensus mechanism should align with specific system requirements and objectives. For IIoT environments seeking to optimize performance and reliability while minimizing energy consumption, PoA represents a promising solution deserving of further exploration and adoption. Ongoing research and innovation in consensus mechanisms will continue to shape the future of decentralized data management, enhancing trust and efficiency in digital ecosystems.

VII. Future Research

Future research could focus on enhancing the security of POA while maintaining its efficiency advantages. While POW offers superior security, POA remains the preferred choice due to its significant edge in speed and energy efficiency. Further exploration into developing consensus algorithms that balance all needs efficiently will contribute to the ongoing evolution of decentralized data management systems, fostering trust and innovation in industrial IoT ecosystems.

References

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

[2] Li, J., Zhang, Y., & Chen, J. (2018). Application of Blockchain Technology in Supply Chain Management. In 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (pp. 1278-1283). IEEE.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp.557–564, 2017.

[4] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized Blockchain for IoT. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 169-174). IEEE.

[5] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” Secur. IT, no. August, pp. 68–72, 2017.

[6] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains,” pp. 1–10, 2018.

[7] Wang, W., Hoang, D. T., Hu, P., Xiong, N., & Niyato, D. (2020). Blockchain for Industrial Automation Systems: A Comprehensive Survey. IEEE Transactions on Industrial Informatics, 16(6), 3902-3912.

[8] P. K. Sharma and J. H. Park, “Blockchain based hybrid network architecture for the smart city,” Future Generation Computer Systems, vol. 86, pp. 650 – 655, 2018.