Industrial Control System State Monitor Using Blockchain Technology

Yun-Hao Chang
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University,
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Tzu-En Peng
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University,
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Jung-Shian Li
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan
E-mail: yhchang@cans.ee.ncku.edu.tw, tepeng@cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw,
ihliu@cans.ee.ncku.edu.tw[*]
www.ncku.edu.tw

Abstract

This paper introduces an innovative approach to enhance data verification and security in intelligent systems through the integration of blockchain technology. The proposed method amalgamates the transparency and decentralization inherent to blockchain with the command and oversight functionalities of PLC to ensure the utmost data integrity. The devised approach synergizes the decentralized attributes of blockchain with the control capabilities of PLCs, thus establishing robust safeguards for data integrity. Through the utilization of blockchain's tamper-resistant ledger, PLCs orchestrate data interactions and enforce real-time monitoring and control. The viability and efficacy of this innovative scheme are substantiated through empirical evaluations and simulations, conclusively affirming its practicality.

Keywords: Industrial Control System, Programmable Logic Controller, Blockchain, State Monitor

1. Introduction

In recent years, with the continuous development of industrial automation, Industrial Control Systems (ICS) have played a crucial role in modern production environments [1]. These systems possess complex architectures, and their proper functioning is paramount to ensuring the stability and efficiency of the production process. However, with the ongoing advancement of digital technology, industrial environments have become more susceptible to data tampering and security threats. Our research is based on the application of blockchain technology, which, with its decentralized and transparent nature, introduces a new level of data security. By integrating blockchain into Programmable Logic Controllers (PLC) ensures the availability and integrity of the data.

2. Related Work

The related work in our study revolves around the application of Industrial Internet of Things (IIoT) and blockchain technology.

2.1. *Industrial Control Systems and Blockchain*

Researchers have explored the integration of blockchain technology with Industrial Control Systems (ICS) to enhance security and privacy within the Industrial Internet of Things (IIoT). Notable studies, such as Z.-H. Sun et al. [2] survey of enterprise and literature reviews to identify specific industrial requirements in various supply chain scenarios, and G. Puthilibai et al. [3] proposal of a secure wireless solution based on blockchain technology for IIoT, and W. Zhou and J. Jin's development and evaluation of a distributed access control system using blockchain and smart contract technologies [4], collectively contribute to advancing the understanding and application of blockchain in the industrial domain.

2.2. *Blockchain Consensus*

Blockchain technology originated from Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" [5] and is a decentralized database technology. Various consensus protocols, including Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), are chosen based on blockchain use cases, performance requirements, and trust levels. The application of PoA (Table. 1) in the Industrial Internet of Things (IIoT) is notable, providing features such as a simplified block verification process, resulting in lower block generation times, and consequently, improved overall efficiency in industrial environments. X. Chen et al. measured the latency performance of Internet of Things (IoT) applications on private Ethereum blockchains, focusing on two consensus algorithms: Proof of Work (PoW) and Proof of Authority (PoA) [6]. The Study show that PoA Ethereum network has a lower Block-Oriented Latency (BOL) than the PoW one due to a simpler block verification process [7].

Table 1. PoA Overview

Energy Efficiency	PoA consumes lower energy compared to other consensuss, making it suitable for applications that demand efficiency.
Transaction Throughput	PoA provides higher transaction throughput, supporting a large volume of real-time transactions, aligning with the needs of industrial control systems.
Applicability	Particularly well-suited for industrial control systems, meeting their strict requirements for efficiency, real-time capabilities, and security.

3. Methodology

3.1. *System Design*

By utilizing Proof of Authority (PoA) blockchain (Fig. 1) [8] as the record framework for the industrial control system. PoA blockchain employs an authority node consensus mechanism where designated nodes are responsible for generating and validating new blocks.

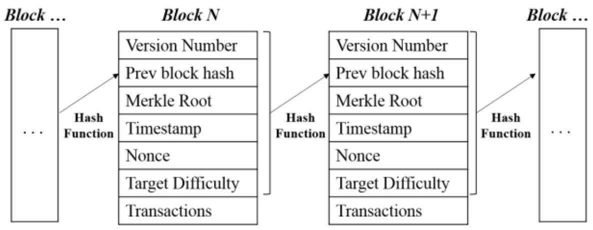


Fig.1. Blockchain Structure

Clients are also participants in the blockchain network, with their primary responsibility being the submission of transactions or information to the blockchain. Clients utilize the Remote Procedure Call (RPC) protocol to communicate with blockchain nodes. This mode of communication allows clients to send remote requests, such as transaction submission requests, while nodes process these requests, participate in the consensus mechanism, and provide feedback on the final outcomes to the clients. (Fig. 2).

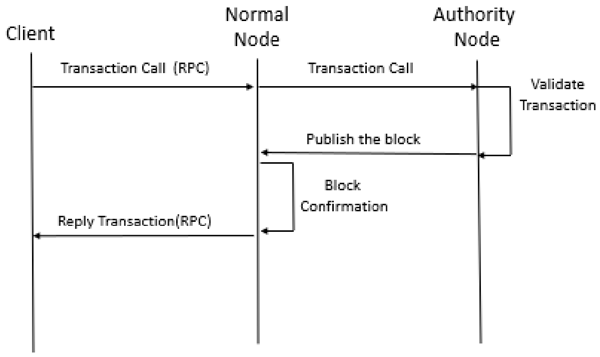


Fig.2. PoA Message Sequence Chart.

3.2. *Data Analysis*

By conducting tests in various scenarios using the same Genesis Block configuration and same mining setting to evaluate our blockchain performance [9]. Firstly, we will explore the multi-node scenario by establishing multiple nodes to simulate a decentralized environment, evaluating the system's performance in a decentralized setting. Subsequently, our focus will shift to the multi-authority scenario, where we increase the number of authority nodes to assess system performance in a multi-authority context. We will emphasize the measurement of Transactions Per Second (TPS) [10], employing different test cases and ensuring experiment repeatability to guarantee result stability. Ultimately, we will present the data distribution using box plots for intuitive comparisons, coupled with statistical analysis to gain deeper insights into the system's performance characteristics under various conditions.

4. Results and Discussion

4.1. *System Simulation*

By emulating the communication between the Human-Machine Interface (HMI) and the Programmable Logic Controller (PLC). The HMI, serving as an authoritative node, is responsible for block generation, transaction verification, as well as establishing connections with the database (DB). On the other hand, the PLC operates as a regular node, handling the synchronization and reception of transactions through client RPC. (Fig. 3).

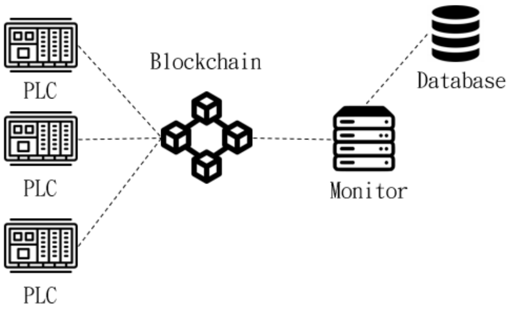


Fig. 3. Integration of blockchain with PLC.

4.2. *Experiment Result*

We measured the service rate variations of a PoA blockchain under the same conditions for other variables (Table 2). Specifically, we assessed the impact of different node counts (from 1 to 3) (Fig. 4) and different validator counts (from 1 to 3) (Fig. 5) on the Transactions Per Second (TPS). Each scenario underwent 30 test iterations, and each test iteration included 1000 transactions.

Table 2. experiment setting

Genesis block	
Period	15 secs
Epoch	30000
Difficulty	0x010
Mining Setting	
CPU	Intel(R) Core(TM) i5-8250U CPU
Thread	1
Software	
PoA blockchain	Geth/v1.10.26-stable-e5eb32ac/windows-amd64/go1.18.5
Client	Nethereum 4.18

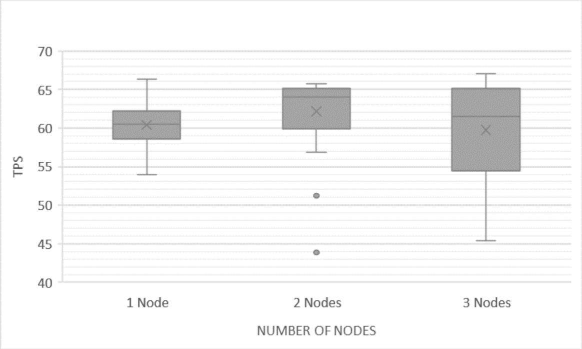


Fig. 4 TPS under different number of nodes

u

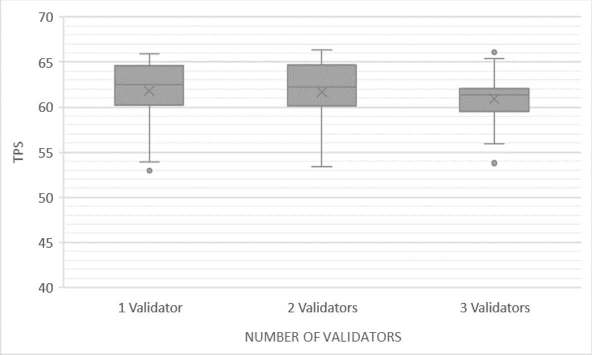


Fig. 5 TPS under different number of validators

The figures above illustrates that there is minimal variation in Transactions Per Second (TPS) across scenarios with 1-3 nodes and 1-3 validators. We hypothesize that the performance of Proof of Authority (PoA) may be more closely associated with the speed of transmission rather than the number of nodes.

5. Conclusion

In this study, we conducted practical experiments on the record-keeping functionality of the Proof of Authority (PoA) blockchain in a real-world Cyber-Physical System (CPS) environment. Additionally, we evaluated the performance of the PoA blockchain under different node counts and validator counts.

In the future, our focus will be on developing a comprehensive blockchain solution for CPS, addressing the undeniable cybersecurity needs of critical infrastructure. We will also continue to monitor the performance assessment of this solution.

Acknowledgements

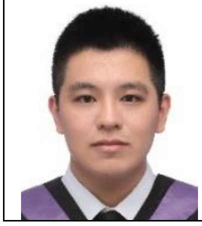
This work is supported by the project from the Water Resources Agency, Ministry of Economic Affairs under contract number MOEAWRA1120307, and the National Science and Technology Council (NSTC) under contract number 112-2634-F-006-001-MBK in Taiwan. The authors sincerely appreciate the assistance provided by them.

References

1. I-H. Liu, K.-M. Su, and J.-S. Li, “The Security Issue of ICS: The Use of IT Infrastructure,” *Journal of Robotics, Networking and Artificial Life*, vol. 8, no. 1, p. pp. 29–32.
2. Z.-H. Sun, Z. Chen, S. Cao and X. Ming, “Potential Requirements and Opportunities of Blockchain-Based Industrial IoT in Supply Chain: A Survey,” IEEE Transactions on Computational Social Systems, vol. 9, no. 5, pp. 1469-1483, 2022.
3. G. Puthilibai, T. Benil, S. Chitradevi, V. Devatarika, D. R. Ashwin Kumar and U. Padma, “Securing IIoT sensors communication using blockchain technology,” 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India ,08 - 09 Dec., 2022.
4. W. Zhou and J. Jin, “A Blockchain-Based Access Control Framework for Secured Data Sharing in Industrial Internet,” 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD), Taiyuan, China, 5-6 Dec., 2020.
5. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 2 Nov. 2023].
6. X. Chen, K. Nguyen and H. Sekiya, “On the Latency Performance in Private Blockchain Networks,” *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19246-19259, 2022.
7. I-H. Liu, Y.-C. Tsai, C.-F. Li and J.-S. Li, “Cross-organizational Non-repudiation Industrial Control Log System Based on Blockchain,” *Journal of Robotics,Networking and Artificial Life*, vol. 9, no. 3, pp. 240-244.
8. C.-H. Wu, I-H. Liu, J.-S. Li and C.-F. Li, “Device's Operation Tracking using Blockchain in Industrial Control System,” ICAROB 2023, Oita, Japan, 9-12 Feb., 2023.
9. M. Schäffer, M. di Angelo and G. Salzer, “Performance and Scalability of Private Ethereum Blockchains,” Business Process Management: Blockchain and Central and Eastern Europe Forum 2019., Vienna, Austria, 1–6 ,Sep., 2019.
10. Y.-C. Tsai, I-H. Liu and J.-S. Li, “Blockchain-based Verification Mechanism for Industrial Control System,” ICAROB 2022, Oita, Japan. 20–23,Jan. , 2022.

Authors Introduction

Mr. Yun Hao Chang



He is acquiring a master’s degree in the Department of Electrical Engineering /Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. His interests are blockchain technology ,and Industrial Control Systems.

Mr. Tzu-En Peng

He is acquiring a master’s degree in the Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. He obtained his B.S. degree from the Department of Electrical Engineering, National Cheng Kung University, Taiwan in 2022. His interests are Cyber-Security and Industrial Control Systems.

Prof. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.

Prof. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests are Cyber-Security, Wireless Network, Group Communication, and Reliable Transmission. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University(TWISC@NCKU).