SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 11(1); May (2025), pp. 78–82
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

Blockchain-Based Monitoring of Industrial Control System

I-Hsien Liu, Yun-Hao Chang, Tzu-En Peng, Jung-Shian Li
National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan

ARTICLE INFO

Article History

Received 31 October 2023
Accepted 25 March 2025

Keywords

ICS
PLC
Blockchain

ABSTRACT

This paper describes an innovative design by using blockchain to improve the verification and security of data in industrial control systems. Combining the decentralized-blockchain, the Programmable Logic Controller, and Human Machine Interface. The design strengthens the overall data security. With the immutable recording function of blockchain, PLC can manage data interactions and conduct real-time monitoring. After testing and simulation, the practicability and effect of this innovative design were proved, and shows the potential of this work.

1 Introduction

This research was prompted by a tragic incident at a dam in Taiwan last year, where a gate unexpectedly opened, releasing 193,440 cubic meters of water without any warning. The sudden flood tragically swept away four campers on the riverbed, resulting in their deaths. Subsequent investigations revealed that the responsible duty officer had neglected their duties and falsified records in the duty log.

To prevent the recurrence of such a catastrophe, this study proposes the integration of blockchain technology with programmable logic controllers (PLC). This integration aims to ensure the availability and integrity of critical data. This innovative establishes a robust framework for securing essential information within industrial environments.

2 Related Works

In the past few years, as industrial automation has advanced, Industrial Control Systems (ICS) have become integral to contemporary manufacturing processes [1]. These systems, characterized by their complex structures, are critical for maintaining the stability and efficiency of production activities. Nonetheless, the increasing digitalization in industrial settings has heightened vulnerabilities to data manipulation and security risks.

Related work revolves around two parts. The first is the industrial control systems, which explores the research on the combination of existing industrial control systems and blockchain applications. The second is the consensus mechanism of blockchain. We compare it in different blockchain consensus mechanisms. And discuss their applicability in industrial control scenarios.

2.1 *Industrial Control Systems*

The integration between blockchain technology and ICS has been a focus of research aimed at bolstering security and privacy in this domain. Key research efforts include Z.-H. Sun, et al.'s review of industrial needs across different scenarios [2], G. Puthilibai, et al.'s design of a blockchain-based secure wireless framework for IIoT [3], and smart contracts for distributed access control.

2.2 *Blockchain Consensus*

In Satoshi Nakamoto's paper [4], he described blockchain as a decentralized, anti-tampering, and a transparent technology. Blockchain have different type of consensus protocols such as PoW, PoS, and PBFT,

Corresponding author E-mail: jsli@cans.ee.ncku.edu.tw

selected based on the specific requirements of the application, including performance and trust levels [5]. Notably, the Proof of Authority (PoA) protocol has been adapted for use in the IIoT [6], offering advantages like reduced block verification time, and explored the latency impacts of PoW and PoA on private Ethereum networks, finding that PoA networks exhibit lower block-oriented latency due to their streamlined verification processes.

3 Methodology

3.1 *Dataset and Preprocessing*

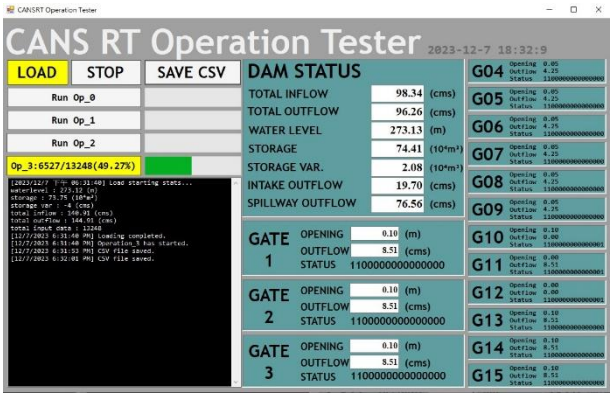

Fig. 1. The Interface of Virtual Dam Gate

This study use the dam gate operating dataset, CANS RT [7], which is a total of 110,000 pieces of information throughout the year including detailed records of water inflow, outflow, the status of the gates, PLC operational states, and other related operational data. We use this dataset for our blockchain record experiments (Fig. 1).

However, in the PoA blockchain transaction content, the data is used to store smart contracts or custom data. This study processes all the data including PLC status, timestamps, inflow/outflow information, etc. into the hexadecimal format, to comply with the data format of within the text section of a blockchain transaction.

3.2 *Data Analysis*

This study conducted a series of experiments under different conditions to evaluate the performance and scalability of our blockchain for industrial control systems. Its process as follow: (Fig. 2)

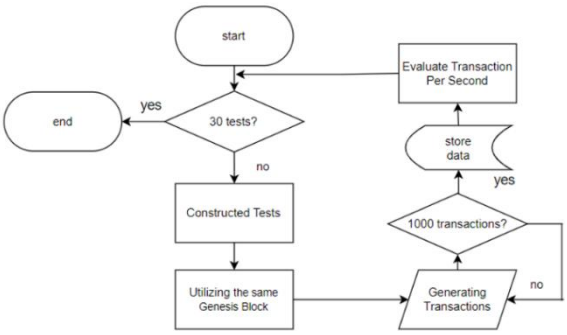

Fig. 2. Data Analysis Flow Chart

The primary indicator of performance was Transactions Per Second (TPS), with test cases employed to verify result reproducibility and consistency. To facilitate a clear comparative analysis, we visualized the data through box plots and performed statistical analyses to examine how the system performed under different configurations.

3.3 *System Design*

In the experiment, we built a PoA blockchain system between HMI and PLC to simulate the ICS system. And there are two main roles in PoA blockchain: authority node and normal node (Fig .3) . In our design, the HMI is designated as an authority node and PLC as a normal node. The HMI responsible of generating new blocks, verifying transactions, and managing connections with the database. At the same time, PLC as a normal node, responsible for synchronizing and forwarding transactions via client Remote Procedure Call (RPC) (Table. 1).

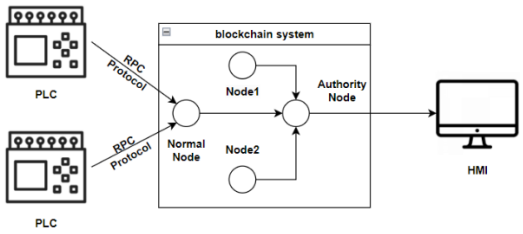

Fig. 3. Blockchain-Based Monitoring System

Authority nodes require high-performance, multi-core processors, large amounts of RAM to quickly process and store transaction data, stable and high-speed network connections, and high-reliability hardware equipment and redundancy. In contrast, normal nodes require a medium-performance processor, a moderate amount of RAM and storage space, and a stable network connection.

Table. 1. The Roles in PoA blockchain

Role	Description
Authority Node	They are responsible for generating new blocks and validating them. These nodes are authorized by the network's management or authority organizations and have the right to validate transactions and create new blocks.
Normal Node	Normal nodes are regular participants in the blockchain network that store complete blockchain data, validate blocks, and propagate transactions. These nodes can submit transactions to the network and accept new blocks.
Client	Clients communicate with general nodes or authority nodes through remote procedure calls (RPC). They establish connections with nodes using network protocols (such as HTTP, WebSocket).

4 Experiment

This study evaluated the system performance by measured TPS with different number of nodes, memory usage, and network usage between authority node and normal node. And the PoA blockchain system setup is listed in Table 2.

Table 2. Experiment Parameters Configuration

Genesis block	
Consensus	Clique
Epoch	30000
Difficulty	0x010
Mining Setting	
Threads	1
Period	15 secs
PLC	
OS	windows embedded standard 7
CPU	1.75 GHz, dual-core
Software	
Geth version	v1.10.26-stable for windows
Framework	.Net Framework 3.5
Nethereum	4.18
others	Grafana, Prometheus

4.1 *Setup*

This study used a PLC with Windows Embedded operating system as a normal node, and another PC as an authority node. By developing a .Net Framework software interface, which read the PLC status and upload the status to the blockchain by using the Nethereum function library.

Additionally, this study used Prometheus and Grafana for monitoring nodes performance, which is a software used to visualized and monitored blockchain node status. Such as transaction speed, node synchronization status, network consumption and memory usage to ensure the operational status of the blockchain.

4.2 *Result*

This study specifically examined the effects of changing the number of nodes (from 1 to 10) (Fig. 4). Conducted 30 test runs for each configuration, with each run processing 1000 transactions. In experiment, we find out that when the number of nodes increases, TPS will gradually decrease.

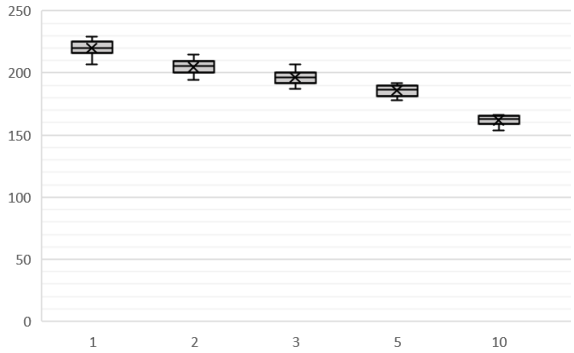

Fig. 4. TPS with Different Number of Nodes

At the same time, this study tested the memory growth of every 10,000 transactions (Fig. 5). The relationship between the number of transactions and the memory growth is found to find the linear growth relationship. Memory usage is around 1 MB per 10,000 transactions.

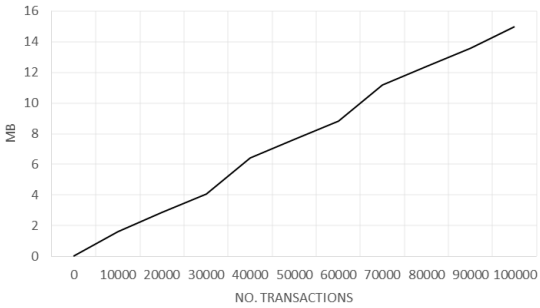

Fig. 5. Transactions Memory Usage

And we use Wireshark to track the network usage between client and authority node, which is around 25~30 KByte/s, which is not a big consumption (Fig. 6).

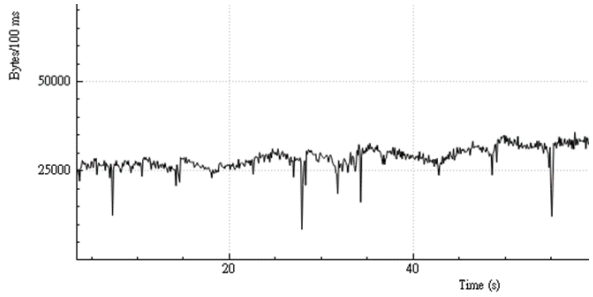

Fig. 6. Network Usage

This study found that the performance of blockchain nodes depends more on hardware resources. In terms of system design, you can use a more powerful CPU, larger memory, increase the maximum number of connections to the RPC server, etc.

5 Conclusion

This research provides a completely PoA blockchain framework to ensure the integrity of industrial control systems. This system not only enhances the security and integrity of data, but also improves the operating efficiency of the system. At the same time, by evaluating the performance of the system, including TPS, CPU usage, network consumption, etc., this provides us with its scalability evaluation of performance and efficiency. Based on the above, we provide a reliable solution for industrial control systems.

Considering the industrial control system, depending on the specific application and design of the system, a typical industrial control system will have hundreds to thousands of sensors, and the amount of data processed per second can reach hundreds of pieces. As This study move forward, our goal is to develop a comprehensive blockchain-based security framework specifically designed for ICS.

This framework aims to significantly enhance the protection of critical infrastructure by leveraging the inherent security features of blockchain technology. In pursuit of this objective, this research will continue to evaluate the effectiveness of our proposed solutions, and hopes to introduce smart contracts, monitoring systems, etc. Focusing on their ability to withstand various cyber threats and ensure robust system integrity.

Acknowledgments

This research is sponsored by the Water Resources Agency (WRA) in Taiwan of the Ministry of Economic Affairs under contract numbers MOEAWRA1120307 and MOEAWRA1130243, and the National Science and Technology Council (NSTC) in Taiwan under contract number 113-2634-F-006-001-MBK.

References

1. I-H. Liu, K.-M. Su, and J.-S. Li, The Security Issue of ICS: The Use of IT Infrastructure, *JRNAL*, Vol. 8, No. 1, 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 Trans. Comp. Social Syst., Vol. 9, No. 5, pp. 1469-1483, 2022.
3. G. Puthilib ai, T. Benil, S. Chitradevi, V. Devatarika, D. R. Ashwin Kumar and U. Padma, Securing IIoT sensors communication using blockchain technology, 2022 ICPECTS, Chennai, India, 08 - 09 Dec., 2022.
4. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 2 Nov. 2023].
5. X. Chen, K. Nguyen and H. Sekiya, On the Latency Performance in Private Blockchain Networks, *IEEE Internet Things J*, Vol. 9, No. 19, pp. 19246-19259, 2022.
6. I-H. Liu, Y.-C. Tsai, C.-F. Li and J.-S. Li, Cross-organizational Non-repudiation Industrial Control Log System Based on Blockchain, *JRNAL*, Vol. 9, No. 3, pp. 240-244.
7. C.-Y. Lee, I-H. Liu, M.-W. Chang, J.-S. Li, 2023, The Dam Gate Cybersecurity Testbed, ICAROB 2023, Oita, Japan, 9-12 Feb., 2023.

Authors Introduction

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, OT Security, and Wired & Wireless Communication. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).

Mr. Yun Hao Chang

He obtained his M.S. degree in 2024 in Computer and Communication Engineering from the National Cheng Kung University, and a B.S. degree in Industrail Engineering from National Tsing Hua University, Taiwan. His interests are industrial 4.0, Cyber Security, ICS and blockchain technology.

Mr. Tzu-En Peng

He obtained his M.S. degree in 2024 in Computer and Communication Engineering from the National Cheng Kung University, and a B.S. degree in Electrical Engineering from National Cheng Kung University, Taiwan. His interests are Cyber Security and ICS.

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.