# Blockchain-based Verification Mechanism for Industrial Control System

**Yao-Chu Tsai** [1]
*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** [2]
*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*** [3]
*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: yctsai@cans.ee.ncku.edu.tw* [1]*, ihliu@cans.ee.ncku.edu.tw* [2]*, jsli@mail.ncku.edu.tw** [3]
*www.ncku.edu.tw*

**Abstract**

Industrial control system (ICS) and critical infrastructure have become increasingly dependent on communication network and cyber-physical systems. Since infrastructure is vulnerable to adversarial attacks, the research on cyber security is vital in Industry 4.0. In order to secure the integrity of data in ICS, this paper proposes a blockchain-based network architecture implemented on physical industrial equipment. By arrangement of blockchain transaction process in the specialized client-server network model, industrial control signal transmission can be verified and recorded based on authority.

*Keywords*: Cyber Security, Blockchain, Verification, ICS Security

## 1. Introduction

With the development of automation and network communication in modern manufacturing technology, the concept of Industry 4.0 has been proposed in recent years, also known as the Fourth Industrial Revolution. The Industrial Internet of Things (IIoT) is one of the widely researched issues. The purpose is to innovate in the industrial economy, construct a smart-conscious industrial environment, and develop smart factories with adaptability, resource efficiency and human-machine collaborative engineering.

Industrial Control System (ICS) contains various kinds of IIoT and critical infrastructure. Security and reliability of ICS has become a concern of industry and government. In 2019, The Department of Homeland Security, United States published “A Guide to a Critical Infrastructure Security and Resilience” to regard critical infrastructure security as national security [1].

As a subgroup of ICS, Supervisory Control and Data Acquisition (SCADA) system is composed of hardware and software related to the data storage, processing, and communication. For instance, Programmable logic controller (PLC) is an operating component in SCADA, which transmits signal among manufacturing equipment and machinery, serving as a fundamental part in cyber-physical system [2].

PLC is basically a terminal device that can control low-level I/O devices, such as sensors or motors, and usually connects to the PC via Ethernet to embed program. As a kind of embedded system on the Industrial Internet, it is exactly at the risk of encountering network attacks. In 2021, a real incident happened in a water treatment plant in Florida. A hacker tried to remotely hack into the water purification control system with an attempt to fill a potentially harmful chemical [3].

In order to ensure the integrity of data transmission and information security, this paper designs a blockchain-based network architecture for the data transmission in industrial control system.

## 2. Background

In this section, we mainly discuss the adaptability of blockchain technique in ICS. Building in the field of industrial networks, the performance of computing equipment in IIoT cannot be compared with that in IT environment. The restriction on IIoT is strict due to transmission time and memory space. Most business owners tend to avoid changing or upgrading hardware because of cost and the possibility of production interruptions [4].

### 2.1. *Modbus TCP*

Modbus is one of the standard communication protocols among PLCs, and it is also commonly used in the current industrial field. Furthermore, Modbus TCP can transmit data through Ethernet TCP/IP. Because Modbus is a plaintext protocol belonging to the application layer, it is easy to be interpreted or tampered by hackers, able to conduct man-in-the-middle attack (MitM) and other malicious behaviors.

### 2.2. *Private Chain*

It is vital to design a secure and efficient network architecture in ICS. Among various types of blockchain, although private chain is a more centralized system, it is quite suitable as a transmission medium for the transfer of confidential value within a single company or organization. Different from public chain and consortium blockchain, only the holder in private chain can participate in the recording of ledgers and data. This factor causes streamlined structure and higher transaction speed of private chain. Therefore, private chain is a better solution for specific institution.

### 2.3. *Proof of Authority*

Proof of Authority (PoA) is a consensus algorithm in blockchain. To obtain the authority, the nodes in the system need to pass the identity verification first. If verified, certain blockchain nodes are set to have the authority to participate in transactions and finally decide whether to add new blocks to the blockchain. In private chain, PoA can makes a positive effect. Compared with proof of work (PoW), PoA does not rely too much on the computing power of network nodes and is more suitable for applications in the environment of industrial control network.

## 3. System Architecture

We make explanation of proposed method and overall framework in this section. There are some adjustments in traditional network configuration and verification mechanism to make blockchain operation more compatible in ICS.

### 3.1. *Network Model*

For the purpose of implementing blockchain in ICS environment, we design a network architecture presented in Fig. 1. It is a client-server network model imported in ICS [5].

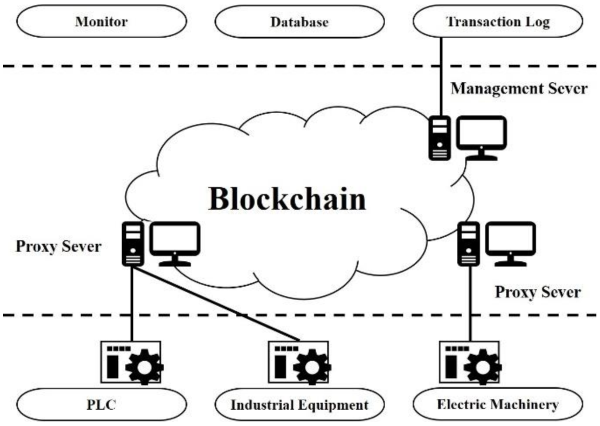

Fig. 1 Blockchain-based ICS network model

The network model explains the ICS devices, such as PLCs, industrial equipment, and electric machinery, are clients of the proxy server. The proxy server accesses to blockchain, so that it can communicate in a protected environment., allocating resources to the ICS devices in the LAN. PC is usually used to be a proxy server, which is more suitable for fast executing blockchain programs in terms of performance.

We propose a method to wrap the Modbus protocol in a block when sending signal using blockchain. Block is a JSON file containing some transaction information, and there is an “extraData” field in it. We decide to put the content of a Modbus packet in this field for transmission in blockchain.

Combined with the immutability property of blockchain, we set a management server to efficiently manage all account information on the network and record the transaction process. If the transaction logs are sealed in the blocks, the log content cannot be easily tampered.

### 3.2. *Blockchain-based Transaction Process*

Having finished registering, we can launch transactions among accounts. The blockchain-based transaction process includes six elements, PLC A, proxy server A, PLC B, proxy server B, and management server. And the whole process can be divided into two phases.

Phase 1: Request from domain A to domain B

- Step 1: PLC A sends Modbus TCP packets to proxy server A to request authentication to access the resources of PLC B.
- Step 2: Proxy server A and proxy server B synchronizes the account information of each other.
- Step 3: Proxy server A initiates a transaction through the blockchain and transfers the Modbus TCP message to proxy server B in the extraData field.
- Step 4: Proxy server B accepts the transaction and signs the certificate by its private key.
- Step 5: Proxy server B takes out the Modbus TCP message in extraData field and sends it to PLC B.

Phase 2: Response from B to A

- Step 6: PLC B sends proxy server B a Modbus TCP packets to make a reply to PLC A.
- Step 7: Proxy server B initiates a transaction through the blockchain and transfers the Modbus TCP message to proxy server A in the extraData field.
- Step 8: Proxy server A accepts the transaction and signs the certificate by its private key.
- Step 9: Proxy server A takes out the Modbus TCP message in extraData field and sends it to PLC A.
- Step 10: Proxy server A and proxy server B synchronize their transaction information to the management server for transaction record backup.

## 4. Experiment

It is practical to choose an appropriate platform according to the required functions in blockchain. Ethereum is used for blockchain development in this paper. The experimental environment setup is shown in Fig. 2.

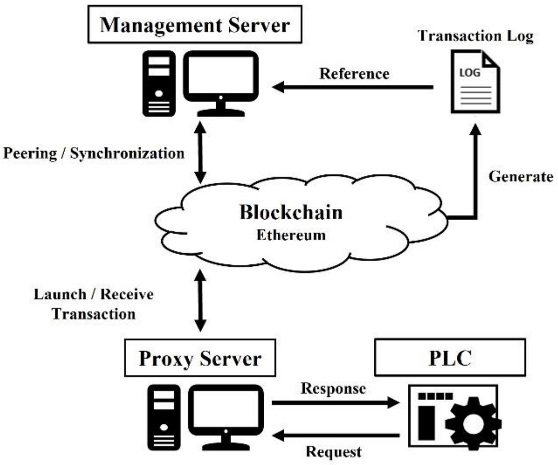

Fig. 2 Experiment environment setup

During online transactions among proxy servers, the Modbus data benefits from the characteristic of security in blockchain. When PLC is ready to receive the verified message, the data needs taking out of the blockchain. As a result, we make an Application Programming Interface (API) to fetch the Modbus information in the block. Likewise, the interface program can also receive signals from PLC. In our experiment, we use the PLC WinPAC WP-8428-CE7 produced by ICP DAS, Taiwan as the industrial control equipment.

Adjusting the block generation period in genesis block, transmission time measurement can be implemented, and the result is shown in Table 1. We found that the period dominates entire transmission time. It can be inferred that when the period is large, the time interval between block generation is also relatively large, which leads to a higher standard deviation of the transaction time.

Table 1. Transmission time with different periods

| **Period (s)** | **Number of Transactions** | **Average Time (s)** | **Standard Deviation (s)** |
|---|---|---|---|
| 1 | 100 | 1.5305 | 0.058719 |
| 5 | 100 | 3.5838 | 0.096524 |

One of application in the management server is transaction log. At the end of each transaction, we arrange for the proxy servers to peer with the management server, synchronizing their transaction logs, so that network administrator can examine all transaction records in convenience by using management server.

## 5. Conclusion

Since the development of information technology is quite rapid, the number and types of IoT devices are increasing. Being a widely used domain of IoT, ICS is constructed by cyber-physical systems. ICS cybersecurity has been a research focus nowadays.

For the purpose of ensuring the transmission integrity in ICS, this paper applies an emerging technology, blockchain, to physical industrial network. Running blockchain in the designed client-server network model, it would improve the adaptability of resource-intensive defense mechanism in ICS.

This paper also plans the transaction process in the blockchain framework, implementing on physical industrial equipment as well. The transaction logs are highly credible and eligible to provide digital evidence since it is not easily tampered. According to the limit and requirement of the environment, we adjust the parameter of blockchain to comply with the coordination of ICS device and IT network management system.

## References

1. F. Enayaty-Ahangar, L. A. Albert, and E. DuBois, “A survey of optimization models and methods for cyberinfrastructure security”, IISE Transactions, vol. 53, no. 2, pp. 182-198, 2020
2. A. Ghaleb, S. Zhioua, and A. Almulhem, “On PLC network security”, International Journal of Critical Infrastructure Protection, vol. 22, pp. 62-69, 2018.
3. CNN, “Florida water treatment facility hack used a dormant remote access software, sheriff says”, https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html
4. G. Bonney, H. Höfken, B. Paffen, and M. Schuba, “ICS/SCADA Security Analysis of a Beckhoff CX5020 PLC”, 2015 International Conference on Information Systems Security and Privacy (ICISSP), 2015.
5. C. Wu, J.Lu, W.Li, H.Meng, and Y.Ren, “Master-slave Blockchain Based Cross-domain Trust Access Mechanism for UPIOT”, 2020 5th International Conference on Computer and Communication Systems (ICCCS), 2020.

## Authors Introduction

Mr. Yao-Chu Tsai

He was born in Pingtung, Taiwan in 1997. He received his B.S. degree from the Department of Systems and Naval Mechatronic Engineering, National Cheng Kung University, Taiwan in 2020. He is acquiring the master’s degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Dr. 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 wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.