A Study on Application of Blockchain Technology to Nuclear Power Plant Control Network

Dongil Lee [a*], Min-Seok Kim [a]
[a]*KHNP, Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, South Korea*
[*]*Corresponding author: diturtle@khnp.co.kr*

1. Introduction

Nuclear Power Plant (NPP) control systems have many types of data (information and control) transmitted and received between systems and facilities. Data integrity is a very important part of data communication, and security has become an important issue in recent years.

So far, it was necessary to examine how to use blockchain technology, unlike the method used for integrity and security of data.

In this paper, we review the block-chain type suitable for the NPP control system, study the private and the public type of the blockchain, and then propose the applicable range and method.

2. Block Chain

This chapter describes the major components of the blockchain and discusses public and private types.

2.1 Blockchain Component

Representative elements of the blockchain include confidentiality, integrity, availability, and anonymity. The following is an explanation of the above important attributes:

- Confidentiality is an attribute of whether a third party can read the encrypted information.
- Integrity prevents forgery and is an attribute to the reliability of the data.
- Availability is an attribute that guarantees user access.
- Anonymity is an attribute that does not disclose the user's personal information.

2.2 Public and Private Types

Public blockchain is a network blockchain like cryptocurrency. Anonymity is a form of emphasis, and forgery is impossible using a distributed system. Decentralization (distribution system) and anonymity are typical attributes.

On the other hand, a private blockchain is a structure that is controlled by a central. Rather than anonymity, it is a way to pre-set participants. [1]

Public blockchain seems like high security because only authorized people can have blocks. However, blockchain security is the opposite because of distributed ledger system. If the data is distributed, forgery is difficult and security is excellent.

The number of blocks (distributed ledger) and security are proportional.

The distributed ledger is on a peer-to-peer network. When a ledger update happens, each node constructs the new transaction, and then the nodes vote by consensus algorithm on which copy is correct. Once a consensus has been determined, all the other nodes update themselves with the new, correct copy of the ledger.

By the distributed ledger system, the blockchain can be modified at any time with the majority consent. Private blockchain has the advantage that they can be easily corrected for bad data. In the case of public blockchain, it is difficult to correct them, which keeps them in the wrong data.

Table I. Private and Public types

	Public	Private
Manager	decdntralized	centeralized
Governance	very difficult change	central authorities can change the rule
Transaction speed	difficult network expansion and slow	easy network expansion and fast
Data access	anonymity	Only authorized users can access
identifiability	anonymity	discernible
Proof of Transaction	PoW, PoS determine the proof of transaction, know who is ahead	Proof of transaction by central authority
Advantage	Ensure safety, reliability, anonymity and transparency	High efficiency and scalability, throughput, Specialization
Disadvantages	Low scalability Slow transaction	Low security

2.3 Blockchain Data Structure

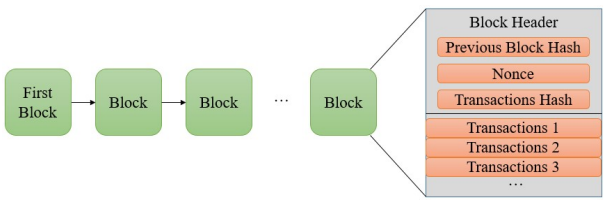

Fig. 1. Blockchain structure

Blockchain can be divided into two sections, header and transaction.

The header contains the previous block hash, the nonce and the current transaction hash, and the transaction contains the records of the transaction. [2]

Table II. Block structure

field	size(byte)	description
Block size	4	Data size from next field to end of block
Block header	80	Information of block header
Transaction counter	1~9	Number of transactions in the block
transactions	Variable	Transactions list

Table III. Block header structure

field	size(byte)	description
Version	4	Software of protocol version
Previous block hash	32	Previous(Parent) block hash
Merkle root (payload hash)	32	Hash of the merkle tree root
Timestamp	4	Block generation time (Unixtime)
Difficulty target (nBit)	4	Block generation PoW difficulty level
nonce	4	PoW count

The important component of the block header is the hash function (SHA-256), which has the following characteristics:

- A function that outputs a fixed length hash value for variable message input.
- If the input is the same, the hash value is the same.
- One-way cryptographic function. (Cannot de-crypto the original value)
- If the input is different, the output value is different in principle.
- The output is the same size regardless of the input.

3. Network of NPP I&C

This chapter describes the information network and control network used in NPP Instrumentation and Control (I&C) network, especially Man-Machine Interface System (MMIS).

3.1 Outline of NPP I&C Network

NPP I&C network uses TCP and UDP communication method based on commercial Ethernet technology. The controllers and servers that make up the MMIS are composed of DCS (Distributed Control System).

The NPP I&C network has high reliability and thorough traffic management compared to the general industrial network, and consists of a redundant information network and a control network according to the characteristics of the network.

3.2 Information Network

The information network consists of several systems of safety and non-safety systems, centering on Information Process System (IPS). The information data of the safety system is own-way transmitted to the IPS of the non-safety system through the gateway, and the various systems of the non-safety system communicate with each other and exchange information.

The information network transmits and receives most of the information of the MMIS, including information related to the safety of the NPP and the status of each system and information for control.

3.3 Control Network

The controller gets the information necessary for the control such as process variables and alarm signals of each system from the information network, and the device control signal processed by the controller is transmitted and received to the devices in the field by the TCP method through the redundant control network.

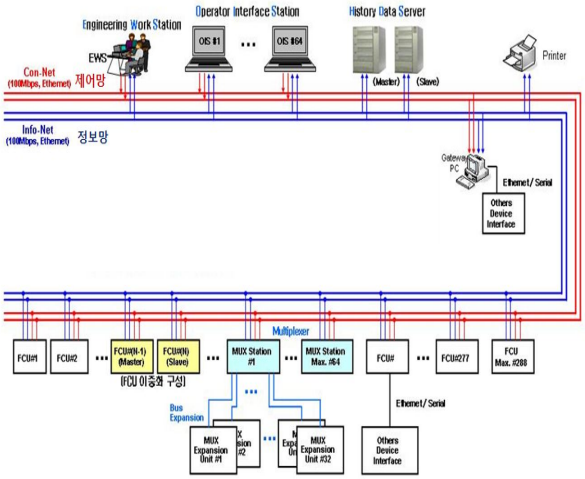

Fig. 2. Non-safety network structure

4. Review of Blockchain Application of MMIS

The application of blockchain to NPP is a very difficult problem and two aspects should be considered.

4.1 Increase Traffic

MMIS of NPP is designed to load 15% of non-safety system and 60% of safety system. [3]

Table III. Traffic of Network

Item	KHNP	WH
Non-deterministic communication (Non-safe)	less than 15% (15Mbps)	less than 60% (60Mbps)
Deterministic communication (safety)	less than 60% (60Mbps)	less than 60% (60Mbps)

In addition, the switch and each server(Drop)/client number is over 500. The non-safety system consists of a tree network of 500 servers/clients. The safety system consists of token-rings network.

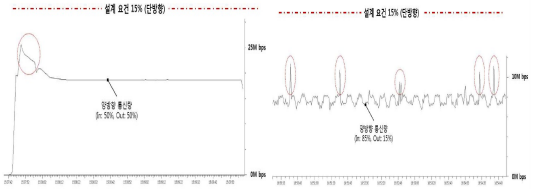

Fig. 3. Control network and control network traffic during normal operation

If the blockchain is configured in the packet, the data load of 1MB or less is added and the load increases by 1MB, which does not significantly affect the design.

However, the load on the failover network increases to the bottom of the design. Figure 4 checks the load during transfer. There is a spare load, but it can have a serious impact if unexpected data congestion occurs.

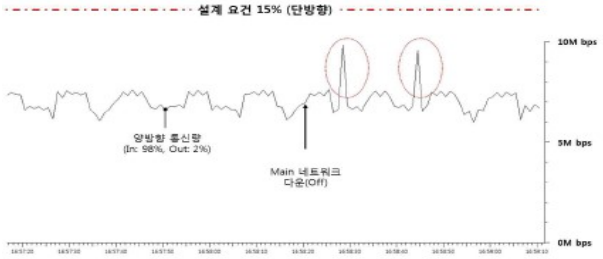

Fig. 4. Network traffic in Failover

4.2 CPU Operation Increase

CPU load in NPP is designed to be less than 60%. Currently, the CPU load rate is under 20 ~ 60%. Memory is also designed for less than 60%. [4]

Table IV. Failover requirements in network

Item	Requirement	condition
Response Time	0.001 ~ 2.5sec	Worst communication situation
Processor Usage	Less than 35-60%	Most stressed anticipated operating conditions
Network Traffic	Less than 15-60%	Worst conditions

In applying blockchain, the CPU load is problem bigger than the network. Getting a nonce requires a lot of CPU resources, even with the help of a GPU.

When a failover or any abnormality occurs, the burden on resources to find a nonce is high. In order to relieve this burden, the difficulty level must be lowered, which results in a fatal result of lowering security.

4. Conclusions

MMIS network is divided into information network and control network. In NPPs, modulation of signals often occurs. This has a huge impact on plant operations.

In addition, there is a part that is neglected in security because of the closed network about cyber security, which is an issue recently. By applying blockchain technology, these parts can be supplemented to the security and integrity of data.

However, it is necessary to develop a technology for reducing the consumption of resources (CPU, memory, etc.) for solving random numbers and for a closed design between switches to reduce network load.

REFERENCES

[1] S. Y. Nam, 블록체인활용기술, 상학당, 2018
[2] A. H. Yoshiharu, 블록체인구조와 이론, 위키북스, 2017
[3] M. G. Min, Evaluation of Non-Safety Network Traffic of Shinhanul Unit #1, Technical Draft, 2019
[4] M. G. Min, Verification of failover effects from distributed control system communication networks in digitalized nuclear power plants, KNS, NET-49-5-11, 2017