Application of Blockchain Technology for Nuclear Industry Cyber Security: A Conceptual Suggestion

Taehoon Kim[a], Moonkyoung Choi[a], Poong Hyun Seong[a*]
[a]*Department of Nuclear and Quantum Engineering, KAIST, Daejeon, Republic of Korea*
[*]*Corresponding author: phseong1@kaist.ac.kr*

1. Introduction

In recent year, digital I&C systems have been developed and installed in operating nuclear power plants (NPPs). However, these changes have problems in terms of security. The digitalization of infrastructure makes systems vulnerable to cyber threats and hybrid attacks. According to ICS-CERT report, as time goes by, the number of vulnerabilities in ICS industries increases rapidly [1].

Recently, due to the digitalization of I&C, it has begun to rise the need of cyber security in the digitalized I&C in NPPs. Many engineers insist that I&C systems of NPPs are physically isolated from external networks so NPPs are regarded safe from external cyber attacks. However, continuous cyber attacks against NPPs are as susceptible to cyber attacks as other critical infrastructures, and public perceptions on cyber security for NPPs have changed [2]. In real, several cyber attacks such as Stuxnet attack, Davis-Besse NPP 'Slammer' worm attack were happened in nuclear industry. These cyber attacks on digital system of NPPs could directly affect the safety, thus the technology for preventing and defending cyber attacks should be developed.

2. Overview of Blockchain technology

Recently, blockchain technology has been attracting attention for security technology. The Blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers [3].

2.1. Blockchain framework

Essentially, blockchain is an underlying technical framework which enables the users to collectively maintain a reliable database in a decentralized manner. As depicted in Figure 1 [3], in a typical blockchain system, data is generated and stored in units of blocks. Consecutive blocks are connected in chronological order to form a chained data structure. All user nodes participate in the validation, storage and maintenance of data. Usually the creation of a new block should be approved by more than half of the users, and broadcasted to all user nodes to perform a network-wide synchronization. Once synchronized, the modify or delete operation is not allowed optionally [4].

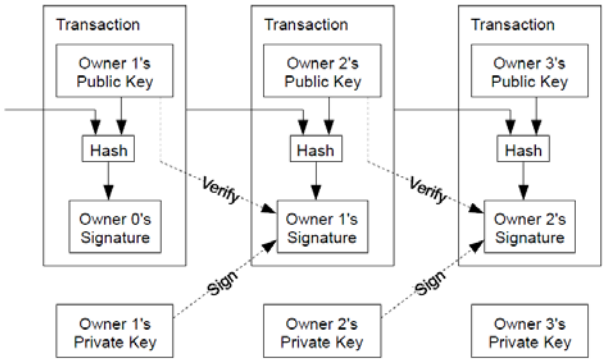

Figure 1. Blockchain technical framework

2.2. Blockchain security advantages

Blockchain has the advantage of tamper-proofing by its unique date structure and data writing mechanism. Once a record is being created in the chained data structure of blockchain, a new timestamp will be recorded at the same time, as depicted in Figure 2 [4]. And any modification of data created before that timestamp will not be allowed any more. In addition, whether a new record can be recorded should be decided by a consensus mechanism. With the existence of the consensus mechanism, the adversaries have to control over half of the network nodes, or possess a stronger computing power to tamper with data in data recording process [4].

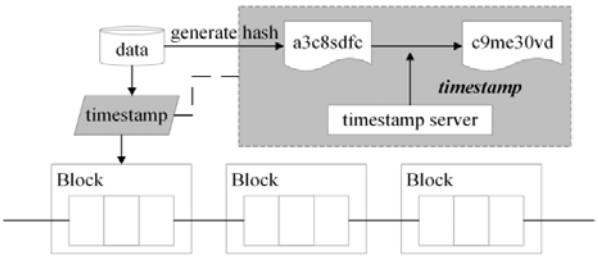

Figure 2. Tamper-proofing mechanism of blockchain

Blockchain also performs data recording and storing synchronously at all users' side. Currently, banks and other security systems are in the form of a central network system. It has the advantage of being simple and fast, but it has a fatal drawback to data security and cyber attacks. Blockchain technology uses a decentralized network system rather than a centralized network. In other words, there is no central point to manipulate the system. All nodes are capable of sending and receiving message to and from each other. Every

node is involved in decision making. This mechanism may cause redundancy to some extent, but reliability and fault-tolerance capability of the network is improved.

2.3. Industry application trend of blockchain

Blockchain was initially put forward as an underlying technical framework of Bitcoin [3]. The basic principle of blockchain is opening, transparency and sharing. By effectively guarantee the authenticity and uniqueness of transaction, blockchain starts to become the technical core of cryptocurrency, asset management, credit control, etc. Furthermore, blockchain gradually exploring its application in financial, medical, energy and ICT fields [4].

3. Application of Blockchain to cyber security in the nuclear industry

To apply the blockchain technology for cyber security in nuclear industry, there are some further points to be considered since the cause and effect of cyber attacks on NPPs are significantly varied [5].

Firstly, the system which can be or should be secured with blockchain technology must be analyzed. Blockchain is very attractive technology to enhance cyber security; however, seen from the application layer, blockchain is still in its exploratory stage [4]. Also, the technology itself still has some inherent security risks. Hence, deep analysis about both system and technology must be done first.

Secondly, proper consensus algorithm should be selected for specific NPP systems. 3 consensus algorithms: Proof-of-Work, Proof-of-Stake, and PBFT (Practical Byzantine Fault Tolerance) are representatives of blockchain consensus algorithms. Each algorithms has pros and cons respectively, so further study about consensus algorithms and matching with suitable NPP system should be done.

Thirdly, data classification and node selection must be done carefully. As mentioned before, in blockchain, all user nodes participate in the validation, storage and maintenance of data. Distributed storage mechanism creates a boarder attack surface in blockchain. In other words, an attacker will have more alternatives to get access to those data. Although content in blockchain is not allowed to tamper, attackers can utilize other techniques to retrieve valuable information [4].

Due to upper reasons, in order to apply blockchain technology for cyber security in the nuclear industry, aforementioned items should be considered.

4. Conclusion

Blockchain technology was initially invented for technical framework of Bitcoin [3]. Because of its advantages in security, many industries are investigating to apply blockchain technology to enhance their cyber security. Cyber security is also an uprising problem in nuclear industry; therefore, can apply blockchain technology to enhance security on specific systems: I&C, nuclear material management system, etc. Meanwhile, several security issues about blockchain are suggested from recent research. Consequently, deep analysis about both NPP system and blockchain technology must be done before to select system effectively and to apply technology efficiently.

REFERENCES

[1] National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, “NCCIC/ICS-CERT Year in Review”, Homeland Security, pp.7-19, 2015

[2] Baylon, Croline, Roger Brunt, and David Livingstone, “Cyber Security at Civil Nuclear Facilities Understanding the Risks”, London: Chatham House, 2015

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2009

[4] Fangfang Dai, Yue shi, Nan Meng, Liang Wei, Zhiguo Ye, “From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security issues”, ICSAI 2017, 2017

[5] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee, “A cyber security risk assessment for the design of I&C systems in nuclear power plants”, Nuclear engineering and technology, Vol.44, No.8, pp. 919-928, 2012