Untact-Era based Modeling for Cybersecurity Using Blockchain Algorithms in Nuclear Industry: A Cyber World Integrity Enhancement in COVID-19 Pandemic

Tae Ho Woo
Department of Mechanical and Control Engineering, The Cyber University of Korea, Seoul 03051, Republic of Korea
**Corresponding author: thw_kor@hotmail.com*

1. Introduction

The block chain algorithm is applied to the 'Information Transfer' to the plant related personnel, which is a kind of cybersecurity matter. So, the 'Unavailability of a system' data can be seen by the personnel securely, that could be used for making a decision with multiple opinions and protecting against possible terrorist's hacking. This concept is described as multiple and secured data transfers in Fig. 1.

Following COVID-19 pandemic, the untact technology is investigated where the blockchain technology has been applied to nuclear industry in which the security as well as safety is particularly important in the industrial aspects. In the information of the nuclear power plants (NPPs), it is possible to be misused for the criminal purposes such as the terrorism. In 2014, the cyber terrorism happened in the commercial South Korean NPP [1]. So, it is needed to transfer the information in NPPs to be treated by the highly advanced secured method. The cryptography as the information security could be representative where the data should be modified following the designed conditions. The Bitcoin has been considered as the cyber-based currency, crypto-currency, which makes a panic to the public in the marketing due to the very high price [2]. It is a kind of technology of the blockchain which is commonly used in crypto-currency [3] in which the hash algorithm is to make the encryption where the information is modified following the designed logic. For the case of the crypto-currency, the price has been regarded as the future trading where it could be changeable very fast. Therefore, the unexpected very high price could be reached.

One of most important characteristics is the merit for accumulations of the information where the block of information is added continuously with spreading to all network connected bodies. So, the information couldn't be changed and the faking is impossible. Hence, the secured industries like nuclear or airplane operations fields need the blockchain algorithm in the data processing. Previously, there are some applications of the blockchain in the nuclear industry. There was a nuclear safety stuff that is considered as the blockchain way [4]. The peer-to-peer business has been considered in the energy industries [5]. Additionally, the nuclear bomb could be protected by the blockchain skills [6]. In this work, the blockchain technology is used to enhance the system integrity in the cybersecurity of NPPs where the cyber performance using the security analysis information is highly enhanced. For the simulations, the blockchain modified modeling is performed with system dynamics (SD) method.

2. Methods

In the NPPs, there are two kinds of important information processing as the security and safety in the systems. Even though the data could be treated as the blockchain logic, the content could be somewhat different. In Fig. 2, the cyber roles are seen in NPPs where the untouchable information is not visible and this cyber space can give the enhanced safety capability in the blockchain method. It is modeled for the cybersecurity of NPPs for the safety analysis information which could be also substituted with the cyber terrorism related information.

The applications of SD by the designed algorithms include the feedback method as one of particular characteristics in SD [7]. A blockchain has been applied to many areas in our lives [8-10]. It is described for the structure of blockchain which is in Fig. 3 [11] where the blockchain structure and blockchain networks are described. The meaning of block includes the hash algorithms where several kinds of hash functions inducing the modular calculations present. One of the hash functions, as an example, could be imagined. That is to say, A mod B produces the remainder value [12]. The previous block means the previous hash. The networking could be connected each other. In addition, it is accumulated by dynamic manner as follows,

$$\text{Block } 1 + \text{Block } 2 + \text{Block } 3 + \cdots\cdots + \text{Block } (n\text{-}1) + \text{Block } (n) \quad (1)$$

Fig. 3 (b) is the arbitrary networking where the block chained information are transferred.

$$A = B = C = D = E = F = G = \cdots\cdots \quad (2)$$

Hence, the networking body is considered as the parallel states where all bodies have same information as equitized positions. Some pieces of event and fault tree could be applied for the modeling in this study. The blockchain modeling is made by the hash function and its block accumulations. In addition, the data are transferred to all connected bodies.

The property of the blockchain is to construct non-centralized operations. For example, in the banking system, the money transaction is just performed by the central control system of the bank. But, in the blockchain system, the information of the financial transaction spreads out to all connected networks. In the case of the Fukushima accident, the golden time to prevent hydrogen explosions had gone away without two treatments as the opening of ventilation value for

hydrogen gas and the cooling by the sea water. The time had passes about one day after earthquake shock induced tsunami that produced the pumping failure by flooding without these treatments. Fig. 4 shows the diagrams for the calculations by Vensim PLE 7.2 code which could be used for the mathematical modeling in science technological and social humanities matters. Fig. 4 (a) presents the diagram of event and fault tree. In Fig. 4 (b) there are some connected operators. This Vensim code is used for the modeling which is in Fig. 4 (a). In Table 1, it is shown the values of each variable are listed. In the case of SCS (safety cooling system) Start Failure, if the randomly generated number is lower than 0.3, the value is 0.0. Otherwise, it is 1.0. It is the typical quantification way in the SD which is based on the random numbers. For Table 2, the modulus is presented as MODULO in Vensim code.

$$\text{MODULO (X, Y) = remainder of X/Y} \quad (3)$$

This function is used for the hash code construction by one of hash algorithms. For the modeling, the accumulations of the event calculation are done in the networking as well as the dynamical state. That is, the level is as follows,

$$Output = \int_o^t Input(t)dt \quad (4)$$

In the application of networking as the blockchain, the discrete values are summed up as,

$$Output = \sum_o^t Input(t) \quad (5)$$

Therefore, the blockchains are accumulated in the modeling incorporated with SD method.

3. Results

In Fig. 5, it is shown for the unavailability by simulations as the conventional with SD and blockchain modified modeling. The blockchain quantifications are done in Fig. 5 (a) for conventional algorithm and SD. The highest value is 2.0 which stands for the worst value of the original tree analysis. There are the comparative values with non-dimension for the unavailability, because the SD was applied in the algorithm. In addition, the encryption is done in Fig. 5 (b), which is obtained by the hash code with the modulus algorithm that the remainder is calculated. For example, in the case of Long-term Conduction which is the highest value as 0.6. If the randomly generated number with 'Recriticality Achieved' is divided by 0.7, the quotient is 2.0 and the remainder is 0.6 at 8th month. This is the configuration of blockchain as follows,

MODULO (if then else (random 0 1 () < 0.3, 0, 1) * Recriticality Achieved, 0.7) (6)

In Fig. 6, there is the diagram for networks simulations for blockchain modified A, C, and G where Fig. 6 (b) is calculated by accumulations as the cumulative unavailability. Using the information of hash code, the decoding could be performed. The networking bodies have same information and can take the secured information. Fig. 7 shows the procedure of the study.

4. Conclusions

It is applied to the nuclear safety for the security reasons using the blockchain technology. Additionally, the cyber security of the NPPs could be improved significantly [13]. In this study, the cyber performance using the safety analysis information is highly improved. So, any kinds of information in the nuclear stuff can be applied using the blockchain technology. For the secured analysis of the nuclear safety, the blockchain method is very effective considering the industrial significance, because the accident could make the unavoidable tremendous damages to the environment such as Chernobyl or Fukushima case. Therefore, the networking based data processing could be the ultimate security technology in the nuclear communities.

For the other applications using the blockchain system, the banking system in already commercialized in some transactions including store businesses. Furthermore, the unmanned car system could be applied where the movements of the automobile are related to the information system of the control monitoring box of the car. It could be utilized in the other unmanned machines like the drone in which the aerial information is transferred to the operations room. In addition, for the military purposes, the crypto technology can be enhanced dramatically. All kinds of information in the communications of the secured data are protected without faking by the networking body where the central control system does not affect on the data communications. Hence, the wiretapping of the sound or image actions are fundamentally prohibited by the property of the blockchain. The blockchain algorithm could be used by the operator to control the anticipated terrorism on the NPPs in which the man-machine relations in the cyberspace could improve the integrity of the operations in the NPPs.

Acknowledgements

This study was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Ministry of Science and ICT (NRF2020M2B5A111090811).

REFERENCES

[1] A. Shalal, IAEA chief: Nuclear power plant was disrupted by cyber attack. Reuters, London, UK, 2016, <https://www.reuters.com/article/us-nuclear-cyber/iaea-

chief-nuclear-power-plant-was-disrupted-by-cyber-attack-idUSKCN12A1OC>.
[2] J.H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle, Secure and anonymous decentralized Bitcoin mixing. Future Generation Computer Systems, Vol. 80, p. 448, 2018.
[3] R.-Y. Chen, A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain. Future Generation Computer Systems, Vol. 80, p. 198, 2018.
[4] Piotrekr, Government should "begin to think" of using Blockchain for nuclear safety, Technology News, 2017, <http://technologynews.site/2017/10/20/governments-should-begin-to-think-of-using-blockchain-for-nuclear-safety/>.
[5] H. Zaremba, Blockchain tech is transforming the energy industry, OilPrice.com, 2018, <https://oilprice.com/Energy/Energy-General/Blockchain-Tech-Is-Transforming-The-Energy-Industry.html>.
[6] J.I. Wong, Even the US military is looking at blockchain technology-to secure nuclear weapons, Quartz, 2016, <https://galois.com/news/even-us-military-looking-blockchain-technology-secure-nuclear-weapons/>.
[7] SDS, What is SD, System Dynamics Society (SDS) Home Office, Albany, USA, 2017.
[8] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommunications Policy, Vol. 41, p. 1027, 2017.
[9] G.J. Larios-Hernández, Blockchain entrepreneurship opportunity in the practices of the unbanked, Business Horizons, Vol. 60, p. 865, 2017.
[10] C. Yang, X. Chen, and Y. Xiang, Blockchain-based publicly verifiable data deletion scheme for cloud storage, Journal of Network and Computer Applications, Vol. 103, p. 185, 2018
[11] M. D'Aliessi, How Does the Blockchain Work? Medium, 2016, <https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae>.
[12] D. Ying, S. Jia, and W. Du, Digital enablement of blockchain: Evidence from HNA group, International Journal of Information Management, Vol. 39, p. 1, 2018.
[13] Woo, Cybersecurity analysis using the blockchain algorithm in nuclear power plants to enhance safe operations. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, xxx, xxx-xxx, 202x.

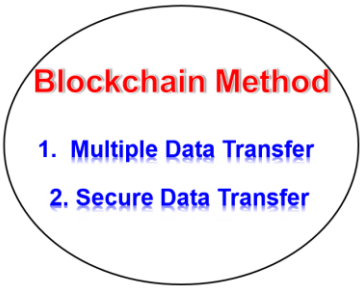


Fig. 1. Concept of bolckchain method.

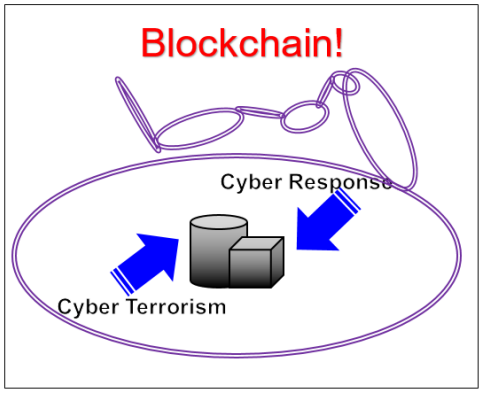


Fig. 2. Cyber roles in nuclear power plants (NPPs).

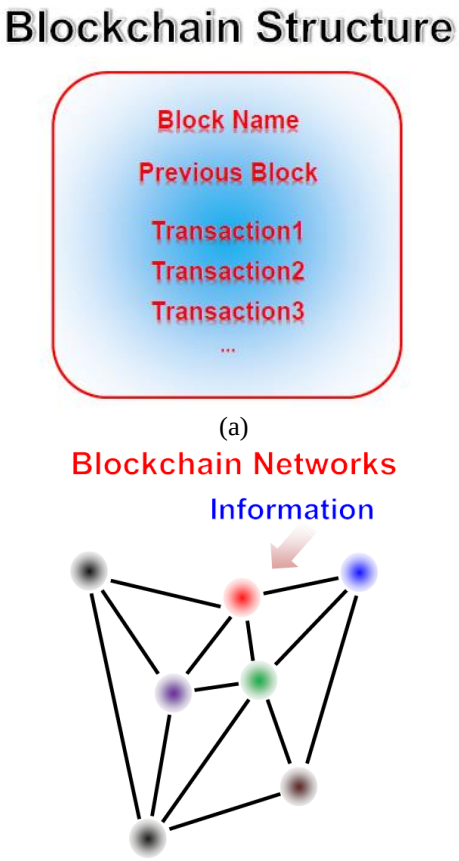
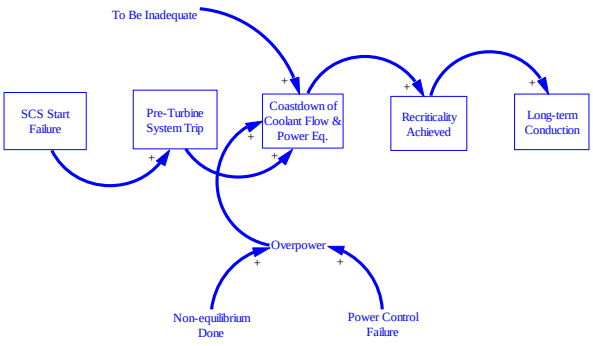
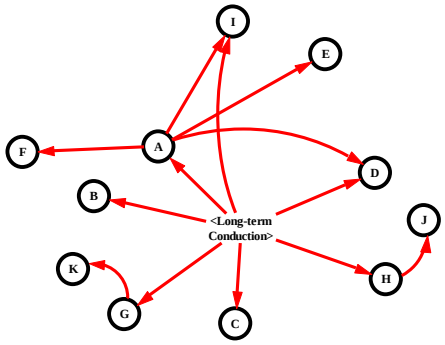


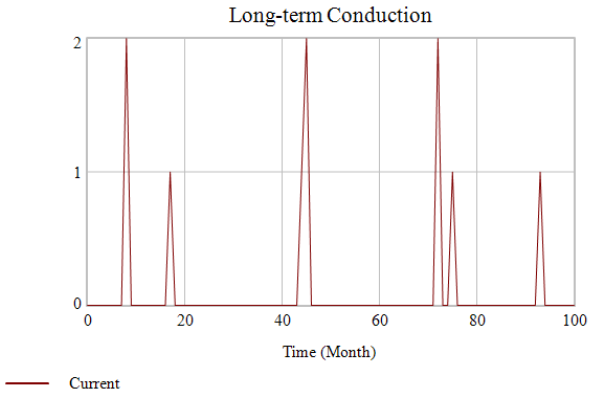
Fig. 3. Blockchain for operations (a) Blockchain structure and (b) Blockchain networks.



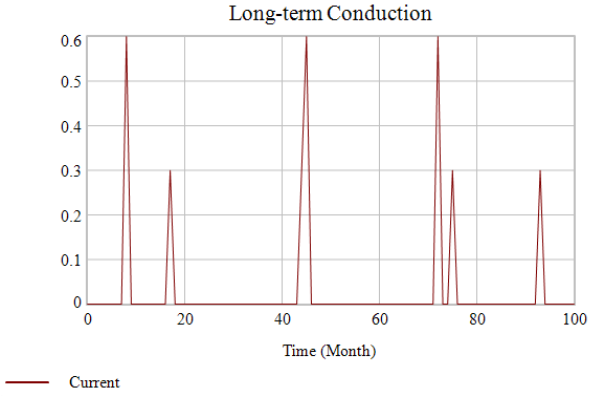


(b)

Fig. 4. Blockchain for operations (a) Blockchain structure and (b) Blockchain networks.

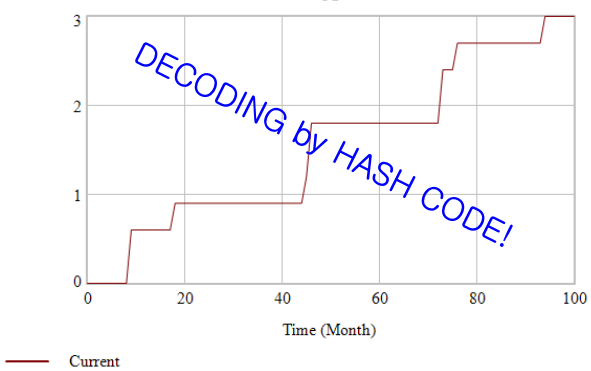


(a)

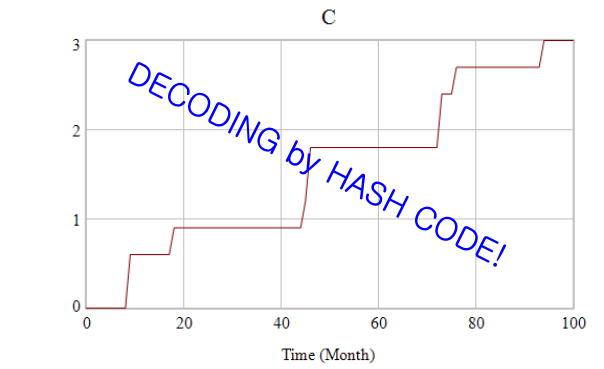


(b)

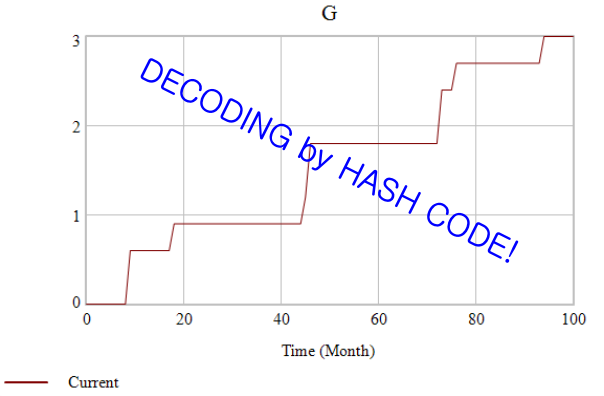
Fig. 5. Diagram for simulations (a) conventional and (b) Blockchain modified.



(a)



(b)



(c)

Fig. 6. Diagram for networks simulations for Blockchain modified (a) A (b) C and (c) G.

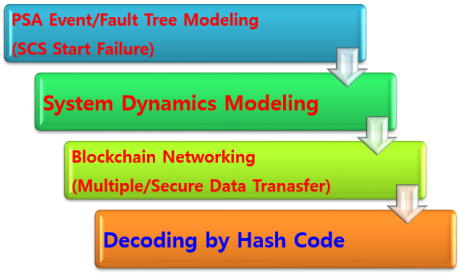


Fig. 7. Procedure of the study.

Table I: List of variables for conventional tree method.

Name	Value
SCS Start Failure	if then else(random 0 1 () < 0.3, 0, 1)
Pre-Turbine System Trip	if then else(random 0 1 () < 0.3, 0, 1) * SCS Start Failure
Coastdown of Coolant Flow & Power Eq.	if then else(random 0 1 () < 0.5, 0, 1) * Pre-Turbine System Trip * (To Be Inadequate + Overpower)
Recriticality Achieved	if then else(random 0 1 () < 0.4, 0, 1) * Coastdown of Coolant Flow & Power Eq.
Long-term Conduction	if then else(random 0 1 () < 0.3, 0, 1) * Recriticality Achieved

Table II: List of variables for block chain modified method.

Name	Value
SCS Start Failure	if then else(random 0 1 () < 0.3, 0, 1)
Pre-Turbine System Trip	if then else(random 0 1 () < 0.3, 0, 1) * SCS Start Failure
Coastdown of Coolant Flow & Power Eq.	if then else(random 0 1 () < 0.5, 0, 1) * Pre-Turbine System Trip * (To Be Inadequate + Overpower)
Recriticality Achieved	if then else(random 0 1 () < 0.4, 0, 1) * Coastdown of Coolant Flow & Power Eq.
Long-term Conduction	MODULO (if then else(random 0 1 () < 0.3, 0, 1) * Recriticality Achieved, 0.7)