Journal of KIIT. Vol. 22, No. 5, pp. 165-171, May 31, 2024. pISSN 1598-8619, eISSN 2093-7571 
http://dx.doi.org/10.14801/jkiit.2024.22.5.165

# 토큰형 블록체인 환경에서의 블록 증명자 추적형 무작위 선출성 강화 메커니즘

김진수*, 박남제**

# Enhanced Mechanism for Randomized Selection of Block Producers with Traceability in Token-based Blockchain Environments

Jinsu Kim*, Namje Park**

이 논문은 2022년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2022S1A5C2A04092269)


## 요 약

기존에는 단일화된 장치 혹은 기기에서 생산된 데이터가 한정된 규모의 네트워크나 단일 기기에서 소비되던 반면, IoT의 활성화에 따라 생성되는 근래의 데이터는 생산된 장치 혹은 기기에서만 소비되는 것이 아닌 외부의 장치에 의한 기록이 가능하도록 변화하고 있다. 수집된 데이터는 사용자 편의성 개선을 위한 데이터로서 활용되고 있다. 특히 단순한 데이터 생성 이외에도 사물에 대한 대여 및 거래, 인증과 같은 다양한 방식으로 활용되고 있다. 따라서 기기에서 생성한 데이터에 대한 무결성 강화가 요구되는 상황이다. 본 논문에서는 블록체인의 블록 증명 권한을 인증하기 위한 수단으로 블록 네트워크 상의 무작위 사용자에게 1회성 블록 증명 권한을 할당하는 토큰이라는 개념을 제시한다. 또한, 토큰이 제 3자에 의해 의도적으로 다른 노드에 전달되는 것을 방지하기 위한 토큰 기반 블록체인 환경을 제안한다.

## Abstract

In the past, data produced from a centralized device or device was consumed in a limited-scale network or single device. However, with the activation of IoT, recent data generated by IoT has changed to be recordable by external devices, not only being consumed by the device itself. The collected data is being utilized as data for improving user convenience. In addition to simple data generation, it is being utilized in various ways such as renting and trading objects, and authentication. Therefore, there is a demand for enhancing the integrity of data generated by devices. In this paper, we propose the concept of tokens, which allocate one-time block validation authority to random users on the blockchain network, as a means to authenticate block validation authority in blockchain. Furthermore, we suggest a token-based blockchain environment to prevent tokens from being intentionally transferred to other nodes by third parties.


Keywords
blockchain, tokens, random rights allocation, integrity, data management

* 제주대학교 사이버보안인재교육원 연구원
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수 (교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

• Received: Mar. 26, 2024, Revised: Apr. 16, 2024, Accepted: Apr. 19, 2024
• Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

## Ⅰ. 서 론

통신 기술이 다양한 영역에 적용됨에 따라 데이터의 무결성 강화는 미래 기술에서의 융합을 구현하기 위해 지속적인 연구가 요구되는 영역이다. 중앙집약형 방식에서 벗어나 분산형 방식을 채택한 블록체인은 거래 원장들을 블록으로 생성하여 이전 블록의 해시를 추가함으로써 데이터의 무결성을 강화하는 한 방법으로 많은 연구가 진행되고 있다. 특히 블록체인은 금전적 거래나 사용자의 인증과 같은 다양한 영역에 적용되어 실제 활용되고 있다[1][2].

일반적으로 블록체인은 PoW(Proof of Work)과 PoS(Proof of Stake) 방식을 적용하여 블록 증명 권한을 할당하는데, PoW 방식의 경우에는 블록 생성을 증명하기 위해 매우 높은 컴퓨팅 파워를 요구하기에 전력 낭비가 심각하다는 단점을 가지고 있다[3][4]. PoS 방식은 자신이 보유하고 있는 지분을 활용하여 블록에 서명하는 방식으로, 컴퓨팅 파워가 상대적으로 낮게 요구되지만 많은 지분을 보유하고 있는 노드에게 높은 수수료를 제공하기에 시간이 지남에 따라 지분을 증명하는 노드가 고착화될 수 있다는 단점을 가지고 있다[5]. 따라서 각 영역에서 블록을 적용하기 위해 최적화된 블록의 검증 방식이 요구된다.

본 논문에서는 상대적으로 적은 컴퓨팅 파워를 사용하여 블록 네트워크에 참여하는 사용자에게 무작위로 블록 증명 권한을 할당하기 위해 토큰이라는 블록 증명 권한을 제공하는 메커니즘을 제안한다. 토큰은 최초에 중앙 서버에 의해 발행되어 블록 네트워크상의 무작위 노드를 선정하여 배포한다. 이후의 토큰은 선정된 노드에 의해 갱신되어 새로운 무작위 노드에게 전달하여 무작위 노드에게 블록 증명 권한을 할당함으로서 지분 증명에 따른 권한 고착화를 방지한다.

## Ⅱ. 합의 알고리즘 분석

블록체인의 합의 알고리즘은 대표적으로 PoW와 PoS 방식이 있으며, 이외에도 DPoS(Delegated Proof of Stake), PoI(Proof of Importance), PoA(Proof of Authority)와 같은 방식들이 존재한다. 본 절에서는 PoW, PoS, DPoS 방식에 대한 분석을 수행한다.

### 2.1 Proof of Work

PoW 방식은 논스(Nonce)라는 임시값을 활용하여 목표값 이하의 블록 해시를 찾는 과정을 수행하여 블록을 생성하고 보상을 획득하는 방식이다. PoW 방식은 노드의 작업량에 대한 증명을 다른 노드에 의해 검증하기에 탈중앙화에 적합한 방식이나, 높은 컴퓨팅 파워를 요구하여 소형 기기에서는 적용이 어렵다. 또한 전력 소비량이 크기 때문에 지속적인 전력 공급이 가능한 환경에 적용이 가능하다[6][7].

### 2.2 Proof of Stake

PoS 방식은 노드의 선정은 무작위로 수행하나, 노드가 가진 지분에 비례하여 선정률이 높아지기에 일반적으로 지분에 따라 의사결정 권한의 획득 가능성이 높은 방식이다[8][9]. 블록의 증명을 위해 노드가 가진 지분을 락업(Lock up)하며, 블록이 성공적으로 추가된 경우에 지분에 따른 보상을 제공한다. 반대로 블록 검증에서 실패할 경우 락업한 지분을 제거함으로써 검증의 신뢰성을 높인다[10]. 따라서 높은 지분을 가진 노드는 손실을 방지하기 위해 블록 네트워크에 기여하여야 한다. 하지만, 이는 지분에 따른 보상을 제공하기에 많은 지분을 가진 노드가 지속적으로 보상을 획득하는 고착화 문제를 야기할 수 있다.

### 2.3 Delegated Proof of Stake

DPoS 방식은 단순히 지분에 따라 블록 증명 권한을 획득하는 PoS와 달리 노드가 자신이 가진 지분을 활용하여 대표 노드를 선정하여 대표 노드가 블록 증명 권한을 할당하는 방식이다[11]. 따라서 빠른 합의가 가능하며, 대표 노드는 일반 노드의 지분을 기반으로 선정되기에 블록 네트워크에 위해를 끼칠 수 있는 대표 노드를 빠르게 다른 노드로 대체할 수 있다[12]-[14]. 하지만 선정된 대표 노드의 과반수가 악의적 노드인 경우에 발생할 수 있는 문제와 대표 노드의 선정을 위한 일반 노드의 참여가 적극적이지 않은 경우 블록 네트워크의 지속적 유지에 문제를 야기할 수 있다는 단점을 가지고 있다[15]-[18].

## III. 기존 연구 분석

### 3.1 토큰형 블록체인 분석

토큰형 블록체인은 토큰 생성 모듈과 블록 검증 모듈의 2가지 모듈로 구성된다[10].

토큰 생성 모듈은 토큰의 생성을 수행하며, 토큰은 토큰 그룹간에 통신을 수행하기 위한 공용키, 블록 검증을 수행하기 위한 비밀키, 토큰을 발행한 생성자 정보, 토큰을 받는 노드 식별정보, 생성시간과 토큰에 대한 해시값으로 구성된다[19]-[21].

토큰은 1차적으로 토큰을 받을 노드의 공개키로 암호화된다. 암호문은 토큰 해시와 토큰 해시를 토큰 내에 포함된 비밀키의 공개키로 암호화한 토큰 해시의 두 가지를 포함하여 토큰 생성자의 비밀키로 암호화하여 블록 네트워크에 배포한다. 따라서 토큰을 받은 검증 노드는 토큰 내에 포함된 비밀키를 사용하여 검증을 증명하고, 새로운 키를 가진 토큰을 발급하여 새로운 노드에게 토큰을 전달한다.

일반 노드에서의 토큰 검증은 토큰을 받은 노드에 의해 토큰 내에 포함된 비밀키로 블록을 증명하였을 때, 토큰 생성 노드에서 받은 토큰 해시와 공개키로 암호화된 토큰 해시를 비교하여 토큰을 증명한 노드가 토큰을 받은 노드임을 증명할 수 있다.

그림 1은 토큰형 블록체인에서의 원장 검증 과정을 보이는 것이다.

### 3.2 토큰형 블록체인의 한계

토큰형 블록체인에서는 거래 원장의 합의 과정에서 토큰이라는 검증용 매체를 사용하여 블록 네트워크에 속한 랜덤한 사용자가 거래 원장 블록을 증명할 수 있도록 한 방식이다.

하지만 토큰의 구성이 토큰을 생성하는 단일 클라이언트에 의존하여 수행되기 때문에 악의적 사용자에 의해 토큰이 조작되는 경우, 특정한 사용자 그룹간에 토큰이 전달되도록 조작할 수 있다는 단점을 가지고 있다. 또한 발행된 토큰의 흐름에 대한 관리 기법이 제시되지 않아 발행된 토큰을 지속적으로 모니터링할 수 있는 방안이 부족하다.

따라서 본 논문에서는 토큰형 블록체인에서 토큰 생성 과정을 악의적인 토큰 생성자가 토큰의 생성에 관여할 수 없도록 한다. 또한, 제 3자에 의한 의도적 개입이 확인되는 경우에 새로운 토큰 그룹을 생성하여 배포하는 방안과 토큰의 지속적인 모니터링 수행을 위한 토큰 추적 방안을 적용함으로서 기존의 토큰형 블록체인의 한계를 극복하기 위한 방안을 제시한다.

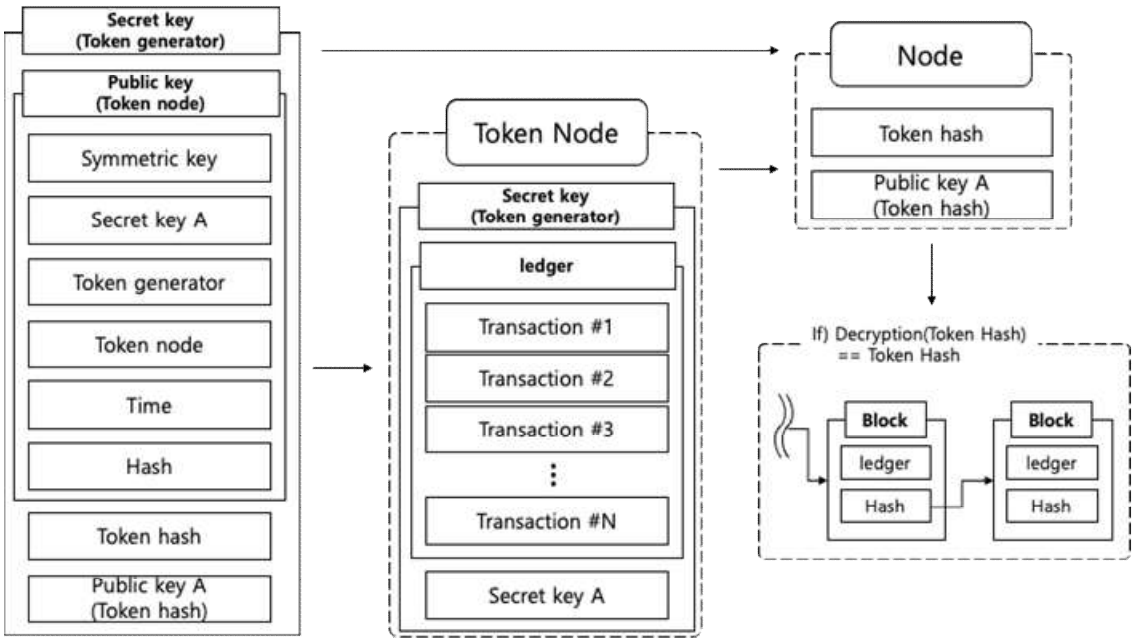



그림 1. 토큰형 분산 네트워크 기반 거래 수행 메커니즘 개요
Fig. 1. Overview of token distributed network-based trading mechanism

## Ⅳ. 토큰 추적형 블록 증명자 무작위 선출 강화 메커니즘

토큰 추적형 블록 증명자 무작위 선출 강화 메커니즘은 기존의 토큰형 블록체인 환경에서의 한계인 토큰 추적 불가와 토큰 생성자에 의한 조작을 방지하기 위해 두 가지 모듈을 제안한다.

토큰의 추적을 수행하기 위해 블록의 생성 과정에서 서비스를 제공하는 서버측에서 토큰을 관리할 수 있도록 하는 토큰 추적 모듈과 토큰 생성 모듈에서 악의적 토큰 생성자에 따른 고착화를 방지할 수 있도록 하는 토큰 무작위 선출 강화 모듈로 구성된다.

### 4.1 토큰 추적 모듈

토큰 추적 모듈에서는 기본적으로 서비스를 제공하는 기관들의 서버를 가정한다. 따라서 서버 간에는 토큰을 획득한 노드의 신원을 증명하기 위해 노드 식별정보의 해시를 공유한다. 그림 2는 토큰 추적 모듈의 전반적인 전개 과정을 보이는 것이다.

토큰 추적 모듈에서의 약어는 표 1과 같다.

표 1. 약어
Table 1. abbreviation

| Abb. | Concept |
|---|---|
| SPK | Server's Public Key |
| SSK | Server's Secret Key |
| TGSK | Token Creator's Private Key |
| TGID | Token Creator's Identification Information |
| TSK | Private Key of Public Key Pair Contained in the Token |
| TNSK | Token Node's Private Key |
| TNID | Token Node's Identification Information |

토큰을 받는 토큰 노드는 서버측으로 토큰을 획득하였음을 증명하기 위해 토큰 해시를 토큰 노드의 비밀키로 암호화하고, 암호문을 다시 서버의 공개키로 암호화하여 블록 네트워크상에 전파한다. 서버는 블록 네트워크상의 노드에게 검증 노드를 증명하기 위해 토큰을 획득한 노드의 식별정보와 토큰의 해시를 서버의 비밀키로 암호화하여 블록 네트워크상에 전파한다. 전파된 해시값은 토큰 노드의 검증에 활용된다.

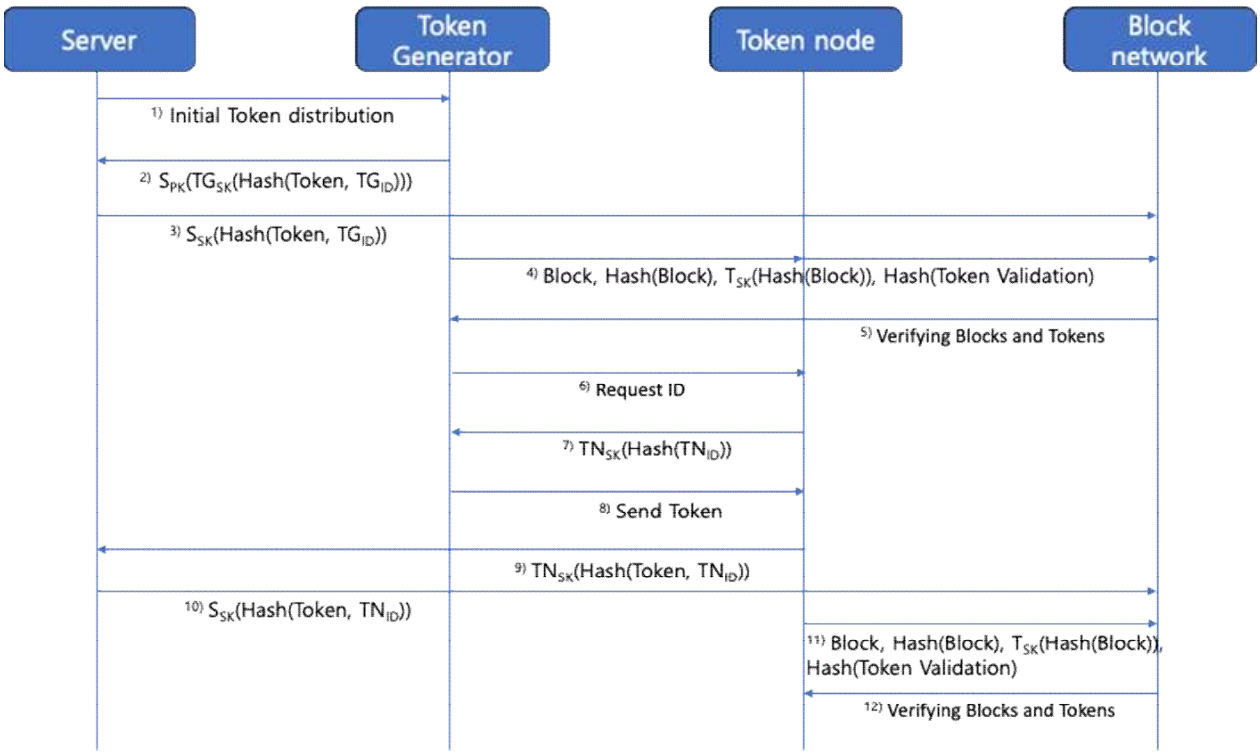



그림 2. 토큰 추적 모듈 흐름도
Fig. 2. Token tracking module flowchart

### 4.2 토큰 무작위 선출 강화 모듈

기존의 토큰형 블록체인에서 블록의 구조는 블록 데이터, 토큰 해시, 토큰 내의 공개키쌍의 공개키로 암호화된 토큰 해시의 3가지로 구성되었다. 하지만 이 경우, 악의적 노드에 의해 임의로 토큰 노드가 선정될 수 있는 위험성을 내포하고 있다.

토큰 무작위 선출 강화 모듈에서는 토큰 생성자 간의 연속성을 증명하기 위해 추가적으로 토큰 생성자 해시를 블록에 추가한다. 또한 각 노드가 블록 네트워크에 참여할 때, 서버에서는 일정한 수의 해시화된 노드 식별정보 리스트를 전송하여 토큰 생성자가 토큰 노드를 선정할 수 있는 리스트를 제공한다.

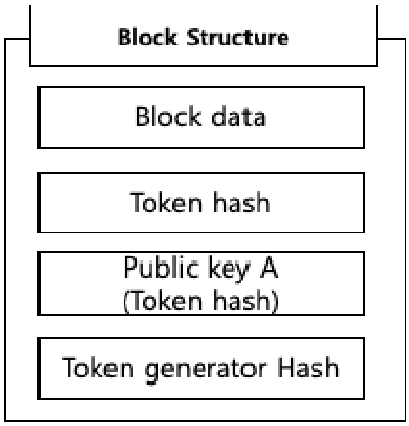



그림 3. 블록 구조
Fig. 3. Block structure

토큰 생성자 해시는 토큰 노드가 새로운 토큰을 발행하는 과정에서 무작위 선출 수행을 위한 것으로, 토큰 생성자의 식별정보 해시와 토큰 노드의 식별정보 해시를 결합하여 새로운 해시값을 생성한 값을 의미한다. 토큰의 선정 과정은 토큰 생성자 해시를 사용하여 노드 리스트의 노드 중 토큰 노드를 선정한다. 토큰을 생성한 토큰 생성자 노드는 직후 새로운 노드 리스트를 서버에 요청하며, 기존의 노드 리스트를 폐기한다. 제안된 방식은 1회성으로 노드에게 제공된 리스트를 사용한다는 점에서 제한적인 무작위 선출을 수행하나, 토큰 생성자에 의한 의도적인 다음 노드 선정을 차단함으로써 악의적인 노드 집단에 의한 고착화를 방지할 수 있다.

## V. 기존 기법과의 비교분석

본 논문에서는 기존의 토큰형 기반 블록체인에서 발생하는 악의적 토큰 생성자에 따른 토큰 생성 무결성의 훼손을 방지하기 위한 방안을 제시하였다.

기존의 토큰형 기반 블록체인은 토큰의 생성 과정이 전적으로 토큰 생성자에게 의존하며, 토큰 생성자에 의해 토큰 내용이 임의로 변경되어도 검증할 수 있는 방안이 존재하지 않았다. 이는 곧 악의적 토큰 생성자가 그룹을 형성하여 블록 네트워크 상의 트랜젝션 증명 권한을 탈취할 수 있는 가능성으로 이어진다. 따라서 토큰의 생성과정에서 토큰 생성자에 의한 임의적 형성을 방지하기 위한 방안이 요구된다.

제안 메커니즘에서는 토큰 생성자는 토큰을 받은 노드의 정보를 포함하여 토큰 노드를 선정하도록 하여 토큰 생성의 연속성을 보장하며, 서버에 의한 1회성 노드 식별정보 리스트를 사용하여 토큰을 선정하도록 하여 토큰 생성자에 의한 임의적 토큰 노드 선정을 방지하였다. 표 2는 제안 메커니즘과 기존의 토큰형 기반 블록체인의 비교분석을 수행한 것이다.

표 2. 제안 메커니즘 비교분석
Table 2. Comparison and analysis of proposed mechanism

| | Token blockchain | Proposed mechanism |
|---|---|---|
| Proof subject | Token | Token |
| Token integrity | Low | High |
| Proof continuity | X | O |
| Token traceability | X | O |

## VI. 결 론

본 논문에서는 기존의 토큰 기반 블록체인 환경에서 토큰 생성이 토큰 생성자에 독립적으로 수행되는 문제를 방지하기 위해 연속성 있는 토큰 생성 방안에 대해 제안하였다.

제안 메커니즘에서는 토큰을 생성할 경우 토큰 생성자가 토큰을 받은 노드의 정보를 포함하여 1회성 노드 식별정보 리스트에서 무작위 노드를 선정

하도록 하여 토큰 생성자에 의한 임의적인 노드 선정을 방지하였다.

하지만 제안 메커니즘은 기본적으로 1회성 노드 식별정보 리스트에 기반하여 노드를 선정하기에 토큰을 생성한 노드는 서버로부터 다시 노드 식별정보 리스트를 받아야한다. 이는 곧 서버의 리소스 요구량이 커진다는 단점으로 이어진다.

향후, 분산 네트워크 환경에서 별도의 서버를 가지지 않고 무작위 증명자 선정이 가능한 메커니즘을 위해 클라이언트 합의에 따른 식별정보 리스트를 생성하는 방안에 대한 연구 수행이 요구된다.

## References


[1] S. J. Yoo, "A Study on Security Enhancement for the Use and Improvement ofBlockchain Technology", Korea Information Assurance Society, Vol. 23, No. 1, pp. 63-68, Mar. 2023. https://doi.org/10.33778/kcsa.2023.23.1.063.

[2] S. H. Son, "Social Change through the Utilization of Big Data and Blockchain based on the Internet of Things in German-speaking countries", Korea and Global Affairs, Vol. 7, No. 6, pp. 459-486, 2023. https://doi.org/10.22718/kga.2023.7.6.018.

[3] J. Kim and N. Park, "De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information", Sensors, Vol. 22, No. 7, Mar. 2022. https://doi.org/10.3390/s22072589.

[4] S. Fahim, S. M. K. Rahman, and S. Mahmood, "Blockchain: A Comparative Study of ConsensusAlgorithms PoW, PoS, PoA, PoV", International Journal of Mathematical Sciences and Computing, Vol. 3, pp. 46-57, Aug. 2023. https://doi.org/10.5815/ijmsc.2023.03.04.

[5] Y. Chen, L. Yang, Y. Fan, L. Zhang, and L. Tien, "Study on energy efficiency and carbon neutral path of Ethereum blockchain: from PoW to PoS", Proceedings Volume 12979, Ninth International Conference on Energy Materials and Electrical Engineering (ICEMEE 2023), Guilin, China, 2023. https://doi.org/10.1117/12.3015149.

[6] N. Sapra, I. Shaikh, and A. Dash, "Impact of Proof of Work (PoW)-Based Blockchain Applications on the Environment: A Systematic Review and Research Agenda", Risk Financial Manag, Vol. 16, No. 4, pp. 218, Mar. 2023. https://doi.org/10.3390/jrfm16040218.

[7] J. Kim and N. Park, "Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments", Applied Sciences, Vol. 10, No.14, pp. 4718, Jul. 2020. https://doi.org/10.3390/app10144718.

[8] M. Wendl, M. H. Doan, and R. Sassen, "The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review", Journal of Environmental Management, Vol. 326, pp. 116530, Jan. 2023. https://doi.org/10.1016/j.jenvman.2022.116530.

[9] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree", Multimedia Tools and Applications., Vol. 80, pp. 34517-34534, 2021. https://doi.org/10.1007/s11042-020-08776-y.

[10] W. Li, S. Andreina, J. M. Bohli, and G. Karame, "Securing Proof-of-Stake Blockchain Protocols", Data Privacy Management, Cryptocurrencies and Blockchain Technology, Vol. 10436, pp. 297-315, Sep. 2017. https://doi.org/10.1007/978-3-319-67816-0_17.

[11] J. Mišić, V. B. Mišić, and X. Chan, "Towards Decentralization in DPoS Systems: Election, Voting and Leader Selection Using Virtual Stake", IEEE Transactions on Network and Service Management, Vol. 21, No. 2, pp. 1777-1790, Apr. 2024. https://doi.org/10.1109/TNSM.2023.3322622.

[12] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using

Character Order Preserving-Transformation in the Emerging Multimedia", Electronics., Vol. 8, No. 4, pp. 412, Mar. 2019. https://doi.org/10.3390/electronics8040412.

[13] C. Li, R. Xu, and L. Duan, "Liquid Democracy in DPoS Blockchains", Proc. of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure, Melbourne VIC Australia, pp. 25-33, Jul. 2023. https://doi.org/10.1145/3594556.3594606.

[14] J. Kim, E. Choi, B. G. Kim, and N. Park, "Proposal of a Token-Based Node Selection Mechanism for Node Distribution of Mobility IoT Blockchain Nodes", Sensors, Vol. 23, No. 19, pp. 8259, Oct. 2023. https://doi.org/10.3390/s23198259.

[15] E. Choi, J. Ko, K. Choi, H. Kim, H. Lee, and N. Park, "Creative convergence course 『Future confluence IT humanities』 development and operational effectivenvess verification", Journal of Korea Multimedia Society, Vol. 24, No. 4, pp. 569-582, Apr. 2021. https://doi.org/10.9717/kmms.2020.24.4.569.

[16] T. Kim, J. Hong, M. Kang, S. Song, J. Lee, and S. Kim, "Integrity Support System for Blockchain-based explainable CCTV Video", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 21, No. 3, pp. 15-21, Jun. 2021. https://doi.org/10.7236/JIIBC.2021.21.3.15.

[17] J. Kim and N. Park, "A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems", Symmetry, Vol. 12, No. 6, pp. 861, May 2020. https://doi.org/10.3390/sym12060891.

[18] J. Kim, D. Lee, and N. Park, "CCTV-RFID enabled multifactor authentication model for secure differential level video access control", Multimedia Tools and Applications, Vol. 79, No. 31, pp. 23461-23481, Jun. 2020.

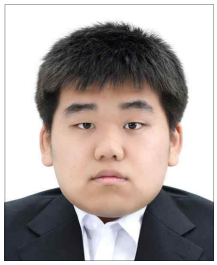
[19] N. Park, J. Kwak, S. Kim, D. Won, and H. Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conferences of Asia-Pacific Web Conference, Harbin, China, pp. 741-748, Jan. 2006.

[20] S. Yoo, "A Study on Consensus Algorithm based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 19, No. 3, pp. 25-32, Jun. 2019. https://doi.org/10.7236/JIIBC.2019.19.3.25.

[21] J. Kim and N. Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing", Personal and Ubiquitous Computing, Vol. 26, pp. 345-353, Aug. 2019.

## 저자소개

### 김 진 수 (Jinsu Kim)



2019년 9월 ~ 현재 : 제주대학교 융합정보보안학협동과정 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

### 박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단
2009년 1월~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드