사물인터넷융복합논문지 Vol. 10, No. 6, pp. 111-116, 2024 https://doi.org/10.20465/KIOTS.2024.10.6.111

블록체인 이중 지불 공격에 적합한 카운팅 블룸 필터를 적용한 DPoS 합의 알고리즘

이수연*
백석대학교 컴퓨터공학부 교수

DPoS Consensus Algorithm using Counting Bloom Filter for blocked Double Spending Attack of Block Chain Attack

Su-Youn Lee*
Professor Division of Computer Engineering Baekseok University

요 약 블록체인 기술의 핵심은 개별 노드들이 자율적으로 블록을 생성하되 일종의 합의과정을 거쳐 결국에는 모든 노드가 같은 블록체인 이미지를 가지도록 하는 탈중앙화방식을 사용한다. 이때 사용하는 기술이 합의 알고리즘이다. 또한 합의 알고리즘은 이중 지불에 대한 문제를 해결하기도 한다. 이를 위해 이용되고 있는 합의 알고리즘인 작업증명(PoW), 지분증명(PoS) 및 위임지분증명(DPoS)을 살펴보았다. 따라서 본 논문에서는 블록체인 공격 중 이중 지불 공격 종류를 살펴보고 이중 지불 공격과 대표자들의 단합을 막기 위해 카운팅 블룸 필터(CBF)를 적용한 DPoS 합의 알고리즘을 제안하고자 한다.

주제어 : 블록체인, 이중 지불 공격, 카운팅 블룸 필터, DPoS 합의 알고리즘

Abstract The core of blockchain technology lies in the fact that instead of a centralized approach, individual nodes autonomously create blocks, but go through a consensus process so that eventually, all nodes have the same blockchain ledger. The technology used in this process is the consensus algorithm. Additionally, the consensus algorithm also helps solve the issue of double spending. To address this, the consensus algorithms used, such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), have been examined. Therefore, this paper aims to examine the types of double-spending attacks in blockchain and propose a Delegated Proof of Stake (DPoS) consensus algorithm incorporating Counting Bloom Filters (CBF) to prevent double-spending attacks and collusion among delegates.

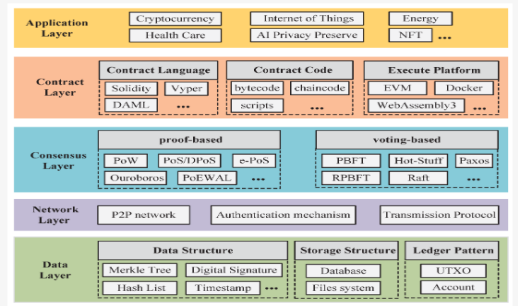
Key Words : Blockchain, Double Spending Attack, Counting Bloom Filter, DPoS consensus algorithm

1. 서론

비트코인(BitCoin)으로 시작된 블록체인은 네트워크에 분산된 개체들이 합의 알고리즘을 사용하여 합의된 블록을 암호학적 해시 함수를 이용하여 추가만 가능하도록 차례로 연결한 분산 원장이다. 블록체인은 암호학적 해시 함수와 전자 서명 등의 암호 기술을 이용하여 구현된다. 블록체인 구성도는 [Fig. 1]과 같다[1]. 블록체인은 분산 컴퓨팅 기술에 기반을 두고 있으며 여러 참여 개체가 동일한 원장을 공유하기 위해 합의 알고리즘을 사

이 논문은 백석대학교 학술연구비 지원으로 작성되었음.
*교신저자 : 이수연(sylee243@bu.ac.kr)
접수일: 2024년 10월 30일 수정일: 2024년 11월 18일 심사완료일: 2024년 12월 03일

용한다. 블록체인 네트워크에서는 일부 노드에 비잔틴 장애를 제외한 일반적인 장애가 발생하더라도 정상적으로 동작할 수 있는 합의 알고리즘이 사용된다. 블록체인에서 사용되고 있는 합의 알고리즘들은 장애 내성, 단위 시간당 최대 트랜잭션 처리량(throughput), 트랜잭션이 변경될 수 없는 상태가 될 때까지 걸리는 시간(time to finality) 등의 관점에서 특성을 비교할 수 있다[2].



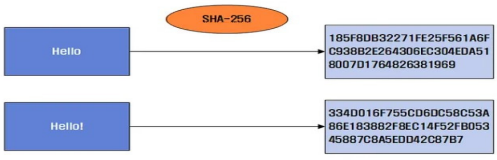
[Fig. 1] Blockchain Architecture

2. 합의 알고리즘 개요

블록체인 기술의 핵심은 특정 노드를 신뢰하지 않으면서 신뢰를 제공한다는 것이기 때문에 중앙집중적 방식이 아닌 개별 노드들이 자율적으로 블록을 생성하되 일조의 합의 과정을 거쳐 결국에는 모든 노드가 같은 블록체인 이미지를 가지도록 하는 방식을 사용한다[3].

2.1 합의 알고리즘

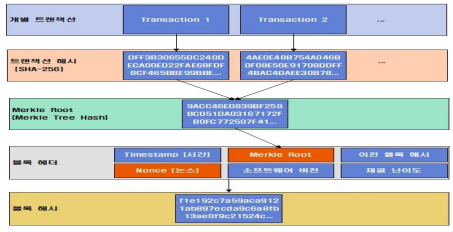
합의 알고리즘을 이해하려면 먼저 해시 함수와 블록 생성 과정에 대해 알아보자. 해시 함수는 임의 길이 데이터를 고정된 길이 데이터로 바꾸는 암호화 함수이다. 비트코인에서는 SHA-256 해시 함수를 쓰는데, 이 함수는 입력 값에 따라 output(해시 값)이 상이하게 바뀐다. 이는 암호화 함수이기 때문에, 해시 값을 가지고 입력 값을 알아내는 것은 무차별 대입을 통한 역추론 방식을 통해서만 가능하다.



[Fig. 2] Hash Function

이 해시 함수를 이용해 트랜잭션 정보를 암호화하고, 블록을 생성한다. 비트코인의 블록 헤더에는 다음과 같은 정보들이 들어간다.

- 블록이 생성된 시간(Timestamp) , Merkle Root
- 이전 블록 해시 : 전 블록과의 연결성을 확보해 블록체인의 불변성 유지
- 현재 소프트웨어 버전
- 채굴 난이도 : 평균적으로 10분마다 한 번 블록이 생성되도록 총 해시 파워에 맞춰 2016 블록마다 한 번씩 조정됨.
- Nonce



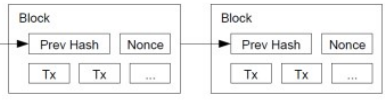
[Fig. 3] Block Generation Process

이 6가지 정보를 이용해 블록 헤더를 다시 해시한 결과를 블록 해시라고 한다. 이 블록 해시를 생성하기 위해 노드들은 경쟁하는데, Nonce가 중요한 역할을 한다. 채굴 난이도에 따라 블록 해시에 대한 기준값이 설정된다. 이 기준값과 비교하여 낮은 값의 블록 해시를 찾아내는 노드에게 블록 생성 권한 및 블록에 대한 보상이 주어진다. 블록 헤더에 들어가는 6가지 값 중 노드들이 임의로 조정할 수 있는 것은 Nonce밖에 없기 때문에 노드들은 Nonce 값을 바꿔가며 무차별 대입으로 기준값 이하의 블록 해시를 찾는다.

2.2 합의 알고리즘 종류

2.2.1 작업증명(PoW: Proof of Work)

PoW는 Satoshi Nakamoto의 논문 “Bitcoin: A Peer-to-Peer Electronic System[4]에 처음 소개되었다. 작업증명에서 채굴이라는 행위를 이해하는 것이 중요하다. 즉, 최초에 Nonce 값을 하나씩 증가하여 채굴된 데이터 값보다 조금 더 작은 해시 함수를 찾는 과정이기 때문이다.

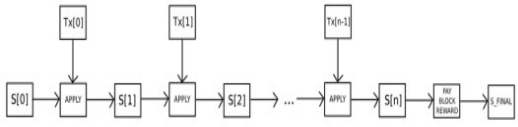


[Fig. 4] PoW function

[Fig. 4]는 하나의 블록체인 노드에 이전에 받은 해시 값과 Nonce 값을 계산하고 보내는 값인 Tx와 받는 Rx 값을 이용하는 블록체인 노드간의 작업을 보여주고 있다. 작업증명은 말 그대로 작업을 많이 하고 암호화를 빠르게 푸는 해시 파워인 것이다. 암호문을 푸는 작업 즉, 마이닝은 10분에 1번 정도 기회가 주어진다. 따라서 합의 시점이 매우 낮아 실제 산업군에 적용하였을 때 너무 낮은 성능이라는 문제점이 발생한다. 즉, 블록 생성이 개별 노드에서 자율적으로 수행되기 때문에 PoW를 통해 랜덤하게 블록을 생성 할 노드를 선택하게 되더라고 같은 부모를 가진 두 개 이상의 자식 블록이 거의 동시에 생성되는 fork가 발생할 수 있다. 이렇게 자주 발생하는 fork는 결국 동일한 블록체인을 가지는 합의에 이르는 것을 어렵게 만들며 합의에 이르렀다 하더라도 가장 긴 체인에 포함되지 못한 많은 블록이 버려지게 되어 시스템 전체의 효율성을 떨어뜨리는 문제가 발생할 수 있다.

2.2.2 지분증명(PoS: Proof of Stack)

PoS 방식은 PoW 방식의 과도한 에너지 소비 문제 해결을 위한 대안으로 제시되었으며 참여자의 소유 지분이 블록 생성권 지분에 반영이 되는 합의 알고리즘이다. 실제도 1초당 약 20회 정도의 합의 과정을 가지고 있다.

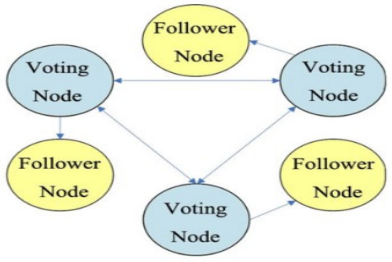


[Fig. 5] PoS function

PoS에서는 마이너가 보유하고 있는 화폐의 양에 비례하여 블록을 생성하게 된다. PoS 개념은 2011년 Bitcountalk 포럼[5]에서 처음 제안되었으며 PoS기반 가상화폐에는 Peercoin, Nxt, Novacoin 등이 있다. 그러나 PoS 방식은 문제는 시간이 지날수록 초기에 지분을 많이 가진 자에게 유리해지는 불평이 발생한다는 것이다. 또한 PoS 방식은 블록 생성 주기를 단축시킬 수 있고 컴퓨팅 파워 낭비를 줄일 수 있어 리소스 관점에서는 효율적이다. 그러나 초기 코인 분배 문제와 아무런 문제가 없다(Nothing at Stake) 문제가 발생할 수 있다. '아무런 문제가 없다' 문제는 유효한 블록체인이 두 개 이상 존재하는 fork 상황에서 참여자들이 보상받을 확률을 높이기 위해 두 개 이상의 블록을 생성함으로써 하나의 블록체인이 수렴해 가는 것을 어렵게 하는 것을 말한다. 이런 상황에서 공격자가 뇌물을 주고 유효한 블록체인을 임의로 바꿀 수 있으므로 유효한 블록체인에 대한 합의를 빨리 이루지 못하는 문제가 발생한다.

2.2.3 위임된 지분증명 (DPoS: Delegated Proof of Stack)

2014년 다니엘 라리머(Daniel Larimer)[6]에 의해 개발된 DPoS 합의 알고리즘은 블록 생성을 위한 노드간의 경쟁방식이 아닌 노드를 미리 지정하여 블록 생성을 하는 방식이다. 노드를 미리 지정하는 방식은 노드 간 투표를 통해 결정되며 선출된 노드들이 블록을 생성할 수 있는 권한이 주어지고 해당 노드들이 생성된 블록의 유효성을 검증하는 합의를 진행하게 된다. 따라서 노드가 미리 정해져 블록을 생성하므로 진행 속도가 빠른 장점이 있다. 단, 거래처리 속도가 빠른 장점이 있지만 블록을 생성할 수 있는 노드들이 공개되기 때문에 해킹의 표적이 될 수 있고 서로 단합할 수 있다는 문제점도 있다.



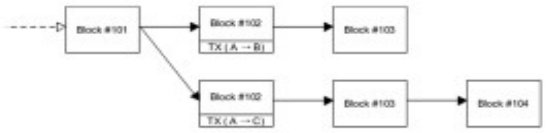
[Fig. 6] DPoS function

2.3 블록체인 공격

블록체인 공격에는 거래소 공격, 지갑 공격, 개인키 복구 정보 공격, 이중 지불 공격이 있다. 이러한 공격 유형 중 이중 지불 공격은 중요도 1-5까지 구분할 때 5에 해당되므로 매우 중요하게 해결해야 하는 공격이다. 즉, 이중 지불 공격은 공격자가 지불된 비트코인을 회수 또는 재지불하여 성공적으로 거래 승인을 완료하고 최종적으로 지불받지 못한 자의 손실이 발생하기 때문이다[7].

2.3.1 이중 지불 공격(Double Spending Attack)

이중 지불은 어떤 트랜잭션이 발생하고 블록에 포함됨으로써 그 블록이 확인된 후에, 공격자가 상충 된 블록을 만들어 네트워크에 전파하고, 빠르게 후속 블록들을 만들어 더 긴 체인을 형성시키면 된다. 블록체인은 항상 가장 긴 체인을 선택하기 때문에 이중 지불이 포함된 블록체인이 정상적인 체인보다 먼저 포함되어 긴 체인을 형성하며 불법 거래가 정상으로 승인된다[8].

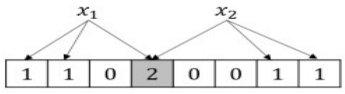


[Fig. 7] Blockchain Fork

이러한 이중 지불 공격은 수신자가 발생된 거래내역의 확인 유무에 따라 미승인형과 승인형으로 구분된다. 미승인형은 수신자가 발생된 거래 내역을 확인하지 않고 이중 지불 된 거래내역을 블록체인에 포함시키므로 정상 지불 거래내역이 블록체인에 불포함되도록 하는 공격이다.

2.3.2 카운팅 불룸 필터

카운팅 블룸 필터(Counting Bloom Filter, CBF)[9]는 블룸 필터의 각 셀이 비트가 아닌 카운터(counter)로 구성된 필터로, 어떤 셀에 원소가 삽입될 때마다 카운트를 1씩 증가시킬 수 있다. 따라서 블룸 필터와 달리 삽입했던 원소를 삭제할 수 있는 기능을 지원한다. 그러나 여전히 거짓 양성이 발생할 수 있으며 실제로는 집합에 포함된 원소를 집합에 포함되지 않았다고 판별하는 '거짓 음성'이 발생할 수 있다.



[Fig. 8] Counting Bloom Filter

3. 이중 지불 공격에 적합한 CBF를 적용한 DPoS 합의 알고리즘

블록체인에서는 다양한 합의 알고리즘을 활용해 블록체인 공격을 방어하려 한다. 특히, 이중 지불로 인한 피해를 막기 위해서는 승인(conform) 수가 일정 수치를 넘어갔는지를 보는 것이 중요하다. 비트코인 기준으로 6개의 승인 이상이 떨어진 트랜잭션에서 이중 지불 문제가 발생할 가능성이 적다는 논문 결과가 나왔다[11].

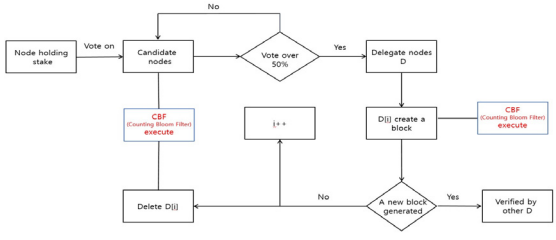
3.1 DPoS 합의 알고리즘

본 논문에서는 블록체인의 공격 유형 중 이중 지불 공격과 대표자의 단합을 막을 수 있는 CBF 를 적용한 DPoS 합의 알고리즘을 제안하고자 한다. 다음은 DPoS의 용어이다.

- 대표자 선출은 참여자들의 보유한 토큰의 수에 비례하여 투표권을 사용하여 대표자 후보에게 투표한다. 모든 투표가 집계된 후 가장 많은 투표를 받은 상위 N명의 후보자가 대표자로 선정된다. 이들은 블록 생성 및 검증 작업을 담당한다.
- 블록 생성 및 검증에서 블록 생성은 선정된 대표자들은 미리 정해진 순서에 따라 블록을 생성하고 각 대표자는 자신의 차례가 되었을 때 네트워크에 전송 된 거래들을 블록에 포함시키고 이를 네트워크에 방송한다. 블록 검증 및 승인은 새로운 블록이 네트워크에 방송되면 다른 대표자들은 이 블록을 검증하고 블록을 승인하면 블록은 네트워크의 공식 블록체인에 추가된다. 보상 분배는 블록 생성 및 검증 과정에 참여한 대표자들은 네트워크에서 정한 보상을 받는다. 이 보상은 대개 새로 생성된 토큰 형태로 제공된다.

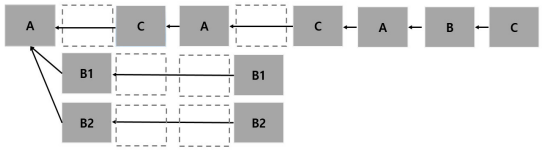
DPoS 합의 알고리즘은 대표자들(Delegated nodes D)에게 과도하게 집중된 권한으로 대표자들이 악의적인 행위 즉, 투표 비용을 지불하거나 자신의 지위를 유지하기 위해 단합하는 경우 네트워크 전체에 심각한 문제를 일으킬 수 있다. 본 논문에서는 DPoS에서 이중 지불 방지와 대표자 간의 단합 문제를 해결하기 위해 CBF를 적용하여 악의적인 대표자를 찾아내어 새로운 대표자를 뽑는 과정을 수행하여 이들의 단합 문제를 해결하고자 한다.

[Fig. 9]는 대표자들이 자신의 지위를 유지하기 위해 단합하는 것을 해결하는 위해 CBF를 적용한 DPoS 알고리즘이다.



[Fig. 9] Operation Process of proposed CBF-DPoS algorithm

[Fig. 10]은 이중 지불이 발생하는 상황이다. 3명의 블록 생산자(A, B, C)가 있고 C를 대표자라고 하자. B가 소수 포크(Minority Fork)일 경우 이중 지불 공격을 할 수 있다.



[Fig. 10] double spending attack

이를 방지하기 위해 B가 블럭을 생성할 때 CBF 셀 값을 1 증가시키게 되면 B가 블록을 재생산 시 다른 대표자들은 CBF 값이 증가 된 것을 보고 블록이 두 번 생산된 것을 알 수 있다. 또한, 선거를 통해 위임받을 대표자가 선출되면 CBF 알고리즘을 수행하여 셀 값을 1 증가시킨다. 또한 대표자로부터 생성된 블록이 검증되지 않으면 셀 값을 1 감소시킨다. CBF를 적용하였을 때 대표자들은 본인이 참여에 대해 선거하는 사용자가 알 수 있기 때문에 서로 단합을 할 수 없게 된다.

3.2 CBF-DPoS 합의 알고리즘 비교 분석

DPoS는 대표로 선출된 대표자들의 3분의 2이상이 동의하면 블록 생성이 완료되는 방식으로 PoS보다 블록 생성과 검증에 동원되는 검증인 숫자를 줄여 속도와 효율성을 높였다.

〈Table 1〉 Comparison and Analysis of Consensus Algorithm

Type	explanation	advantage	disadvantage
PoS	•Ownership-Based •Equity-Based •Theoretical Excellence	•51% Tolerance •Fast Transaction	• Lack of Integrity •Lack of Verification
DPoS	•Delegated PoS •Excellent Transaction Speed •Validated Trust Dependency	•51% Tolerance •Fast Transaction •Energy Saving	•Lack of Integrity: •Lack of Verification •Security Weakness
CBF-DPoS	•Delegated PoS •Excellent Transaction Speed	•Fast Transaction •Verification Enhancement •Security Enhancement	•Lack of Integrity

또한, 채굴기나 디지털자산 등 많은 자본을 가진 사람이 모든 것을 다 결정하는 PoS에 비해 코인 보유자들이 자신의 권한을 위임해 대표자를 선출한다는 측면에서 좀 더 민주주의적이라고 할 수 있다. 그러나 DPoS는 네트워크 최선의 이익을 위해 행동하는 대표자에 의존하므로 대표자들이 단합할 위험이 발생하므로 보안에 취약하다. 따라서 〈Table 1〉에서와 같이 DPoS의 문제인 보안 취약 문제를 CBF-DPoS에서 대표자들의 블록 생성 시 셀 값을 1 증가시키고 블록 삭제 시 셀 값을 감소시키므로 생산자들이 그 셀 값을 보고 확인 할 수 있으므로 이중지불 및 대표자 단합을 해결하여 보안 측면 및 검증 부분을 향상시켰다.

4. 결론

본 논문에서는 비트코인(BitCoin)으로 시작된 블록체인의 개념과 핵심 기술인 합의 알고리즘에 대해 살펴보았다. 이러한 블록체인은 어떠한 합의 알고리즘을 사용하는지에 상관없이 공격에 취약하다는 문제점을 가진다. 따라서 본 논문에서는 블록체인 공격 중 가장 피해를 많이 주는 이중 지불 공격을 방지하면서 대표자들의 단합 문제를 해결하는 카운팅 블룸 필터(CBF)를 적용한 DPoS 합의 알고리즘을 제안하였다. 추후 연구 과제로는 CBF-DPoS 합의 알고리즘 성능을 시뮬레이션을 통해 증명하므로 실제 서비스에 사용할 수 있도록 연구하고자 한다.

REFERENCES

[1] W.Deng,T.Huang and H.Wang, "Review of the Key Technology in a Blockchain Building Decentralized Trust Platform", Mathematics, 2023.

[2] V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM," pp.12-16, 2017.

[3] J.C.Lim and N.S.Ko, "Generational Blockchain Consensus Algorithms", 2020.

[4] S.Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," pp.10-14, 2008.

[5] C. Osborne, "Bitcoin Gold suffers double spend attacks, $17.5 million lost," ZDNet, 2018.

[6] S.K Kim, U.M Kim & J.H Huh, "A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security," MDPI Energies Vol.12, No.3, pp.120-125, 2019.

[7] R.C.Park and Y.S.Lee, "An Overview of Blockchain Technology: Concepts, Consensus, Standardization, and Security Threats ", Dec. 2019.

[8] J.S.Lee, "A methods for attack a blockchain through double spending", Trend Games, 2018.

[9] A. Broder and M. Mitzenmacher. "Network applications of Bloom filters: A survey. Internet Mathematics", Vol.1,No.4, pp.485-509, 2004.

[10] B. Chazelle, J. Kilian,R. Rubinfeld and A. Tal,"The

bloomier filter: an efficient data structure for static support lookup tables," in SODA '04: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, (Philadelphia, PA, USA), Society for Industrial and Applied Mathematics, pp.30-39, 2004.

[11] M.J.Shin, W.W.Kim, Y.J.Kang and H.J.Seo, "The trends of Blcokchain technology in the of IoT", Journal of Information Security, 2022.

[12] Z.Hussein, M.A. Salama1 and S.A.E.Rahman "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms, Hussein et al. Cybersecurity, 2023.

[13] R.Yousuf and Z.Jeelani "Consensus Algorithms in Blockchain-Based Cryptocurrencies",ICAECT, 2021.

[14] S.Zhang & J.H.Lee, "Analysis of the main consensus protocols of blockchain", Vol.6, No 2, pp.93-97, 2020.

[15] J.Yusoff1, Z.Mohamad1 and M.Anuar, "A Review: Consensus Algorithms on Blockchain", Journal of Computer and Communications, Vol.10 No.9, September 2022.

[16] K.Kim, Y.Jeong, Y.Lee and S.Lee, "Analysis of Counting Bloom Filters Used for Count Thresholding", Electronics, 2019.

이 수 연(Lee Su Youn) **[정회원]**

- 1991년 2월 : 단국대학교 전자계산학과(이학사)
- 1993년 2월 : 단국대학교 전산통계학과(이학석사)
- 2004년 2월 : 성균관대학교 전기전자컴퓨터공학부(공학박사)
- 1997년 3월 ~ 2024년 2월 : 백석문화대학교 컴퓨터공학부 교수
- 2024년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
사물인터넷, 블록체인, 암호 프로토콜, 정보통신