Journal of Digital Convergence
Vol. 17. No. 12, pp. 219-228, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.12.219

에지 컴퓨팅 기반의 사물인터넷에 대한 블록체인 적용 방안 연구

최정열
성결대학교 컴퓨터공학과 부교수

A study on the application of blockchain to the edge computing-based Internet of Things

Jung-Yul Choi
Associate professor, Department of Computer Engineering, Sungkyul University

요 약 정보기술의 발달과 스마트한 서비스의 활성화로 인해서 다양한 스마트기기가 네트워크에 연결되는 사물인터넷 기술이 지속적으로 발전해오고 있다. 기존의 사물인터넷 구조에서는 클라우드 컴퓨팅 기술을 기반으로 중앙 집중형으로 데이터를 처리해왔으나, 단일 장애 지점, 종단간 전송 지연, 보안에 대한 우려가 있다. 이러한 문제를 해결하기 위해서 탈중앙화된 블록체인 기술을 사물인터넷에 적용할 필요가 있다. 하지만 많은 사물인터넷 기기들은 컴퓨팅 성능이 부족하여 블록 채굴과 같은 막대한 자원이 소요되는 일을 처리하기에 어려움이 있다. 이를 극복하기 위해서 본 논문은 컴퓨팅 자원이 부족한 사물인터넷 기기에서도 블록체인 기술을 적용할 수 있는 에지 컴퓨팅 기술 기반의 사물인터넷 구조를 제안한다. 본 논문은 또한 에지 컴퓨팅 기반의 사물인터넷에서의 블록체인의 동작 절차를 제시한다.

주제어 : 블록체인, 사물인터넷, 에지컴퓨팅, 포그 컴퓨팅, 합의알고리즘

Abstract Thanks to the development of information technology and the vitalization of smart services, the Internet of Things (IoT) technology, in which various smart devices are connected to the network, has been continuously developed. In the legacy IoT architecture, data processing has been centralized based on cloud computing, but there are concerns about a single point of failure, end-to-end transmission delay, and security. To solve these problems, it is necessary to apply decentralized blockchain technology to the IoT. However, it is hard for the IoT devices with limited computing power to mine blocks, which consumes a great amount of computing resources. To overcome this difficulty, this paper proposes an IoT architecture based on the edge computing technology that can apply blockchain technology to IoT devices, which lack computing resources. This paper also presents an operaional procedure of blockchain in the edge computing-based IoT architecture.

Key Words : Blockchain, Internet of Things, Edge computing, Fog computing, Consensus algorithms

1. 서론

정보기술의 발달은 사회 전반에 걸쳐서 여러 가지 변화를 가져오고 있다. 특히, 인터넷을 기반 구조로 하여 각종 기기들, 예를 들어 센서, 냉장고, 셋탑박스, TV, 스마트폰, PC, 자동차, 등이 연결되는 사물인터넷이 주요 기술로 활용되며, 4차 산업혁명의 핵심 기술로 손꼽히고 있다. Cisco에 따르면 각종 사물인터넷의 기기 간 연결은

*Corresponding Author : JungYul Choi(passjay@gmail.com)
Received October 14, 2019 Revised November 29, 2019
Accepted December 20, 2019 Published December 28, 2019

2017년 61억에서 2022년에는 146억으로 2.4배가 증가할 것으로 예상되는 바[1], 그 활용성과 중요성이 가중되고 있다.

현재의 사물인터넷 구조에서 각종 센서 및 스마트기기로부터 입수되는 데이터 및 정보들은 클라우드 컴퓨팅 장치에서 처리된다. 이러한 중앙형 처리 구조는 대규모의 컴퓨팅 자원을 이용해서 효과적으로 정보를 처리할 수 있다는 장점은 있으나, 장애 발생 시 파급 효과가 크며, 종단간 전송 및 처리 지연이 발생할 수 있다는 단점도 존재한다[2,3]. 자율주행 자동차와 같이 초저지연 통신을 요구하는 서비스의 경우에는 지연 시간 감축을 위해서 중앙형 클라우드 컴퓨팅 대신에 포그 컴퓨팅과 같은 에지 컴퓨팅 기술을 활용하고자 많은 연구가 진행 중이다[4,5]. 에지 컴퓨팅은 사용자의 요구에 더 빠른 응대를 할 수 있도록 네트워크 가장자리에서 컴퓨팅 자원을 제공하는 클라우드 서비스를 제공한다[4].

한편, 사물인터넷에서는 각종 센서 및 스마트기기로부터 개인정보를 포함한 다양한 정보와 데이터가 발생하기 때문에, 개인정보 유출과 보안에 대한 우려가 매우 크다[2]. 특히, 클라우드 컴퓨팅 기반의 구조에서는 데이터 추적 및 관리가 어려우며, 단일 장애 지점으로 인한 장애 대책이 요구된다. 이에 대한 보완 대책으로 최근에 블록체인 기술을 활용한 탈중앙화된 사물인터넷 기술이 주목을 받고 있다. 분산 원장 기반의 블록체인 기술은 기본적으로 P2P(Peer-to-Peer) 기반의 분산형 네트워크 구조를 갖기 때문에 단일 장애 지점에 대한 우려가 없으며, 중앙 서버로의 병목 방지, 통신 중인 데이터에 대한 무결성 및 위변조 방지 보장, 그리고 데이터 추적이 용이한 장점을 제공한다[2,3,6,7].

블록체인 기술을 적용하기 위해서는 각 피어들이 트랙잭션에 대한 검증 및 블록 생성에 대한 책임이 있다. 특히, 블록을 생성하는 과정에서 작업 증명 등과 같은 합의 알고리즘을 적용할 때 막대한 양의 컴퓨팅 자원을 소비하기 때문에 자원이 제한적인 사물인터넷에서의 기기에 곧바로 적용하기에는 어려움이 따른다[2,8]. 이에 따라 사물인터넷에 블록체인을 적용할 때, 사물인터넷 기기의 성능 및 컴퓨팅 능력에 따라 풀 노드(full node), 가벼운 노드(light node), 또는 트랜잭션만 생성할 수 있는 등 역할을 달리 하거나[2,9], 사물인터넷 게이트웨이를 활용하거나[10], 또는 에지 컴퓨팅 장치로부터 필요한 자원을 빌려서 블록체인에 참여할 수 있다[3,8].

본 논문은 컴퓨팅 자원이 불충분한 사물인터넷 기기가 블록체인 네트워크에 참여하도록 에지 컴퓨팅 기술을 활용한 사물인터넷 구조에서의 블록체인 적용 방안에 대해서 살펴본다. 본 논문은 다음과 같이 구성된다. 2장에서는 블록체인의 동작방식 및 종류, 그리고 합의 알고리즘 등 블록체인의 개요를 소개한다. 3장에서는 사물인터넷에 블록체인을 적용하려는 선행 기술에 대해서 분석한다. 4장에서는 에지 컴퓨팅 기술에 대한 소개, 에지 컴퓨팅 기반의 사물인터넷-블록체인 결합 구조, 그리고 블록체인의 동작 방안에 대해서 소개한다.

2. 블록체인 개요

2.1 블록체인의 동작 방식

블록체인은 전자서명, 해시함수 등 암호화 기술을 이용하는 암호화폐인 비트코인을 지원하기 위해서 개발되었다[11]. 중앙의 관리자가 없이도 공개된[1] 네트워크에 참가한 사람들에 의해서 생성된 거래 내역이 참임을 증명하는 것에 대해서 합의를 이룰 수 있고(따라서 '분산형 합의'라 한다.), 모든 거래 내역을 추적할 수 있으며, 한번 거래된 내역을 위변조하기 어렵다는 장점을 지니고 있다. 분산되고 독립적이며 개방된 원장 관리의 장점으로 인해서 암호화폐 이외에도 에너지, 수송, 물류, 헬스케어, 금융, 스마트시티 등 다양한 응용으로 그 쓰임새가 확대되고 있다[3].

블록체인 기술은 중앙의 관리자 또는 감시자가 없이 동등한 역할의 참여자들로 구성된 P2P(peer-to-peer) 네트워크 상에서 구현된다. 참여자들이 생산하는 거래 내역(또는 트랜잭션)이나 데이터들은 모든 참여자들 간에 서로 공유된다. 생성된 트랜잭션이 유효하려면 블록에 포함이 되어야 하며, 이 과정을 '채굴(mining)'이라고 한다. 트랜잭션이 블록에 포함되는 과정은 다음과 같다. 먼저 참여자들은 자발적으로 P2P 네트워크 상에서 새롭게 생성되어 유통되는 트랜잭션의 정상 유무를 검증한다. 정상적인 트랜잭션으로 판명이 되면 블록에 추가하게 된다. 하나의 블록에는 여러 트랜잭션들이 포함될 수 있다. 블록은 누구나 생성할 수 있지만 가장 먼저 생성한 블록만 유효하다. 예를 들어, 어떤 트랜잭션이 A라는 블록에 포함되어 생성되었는데, 바로 뒤에 다른 참여자에 의해서 블록 B에도 포함이 될 수 있지만, 참여자들 간의 합의에

1) '공개된'이라는 의미는 누구나 참여할 수 있다는 의미로, 중앙의 관리자 등 제 3자에 의한 참여 허가를 받을 필요가 없다는 뜻이다.

의해서 늦게 생성된 블록B는 무효화된다(합의 과정은 2.3절에서 상세하게 설명한다.). 블록을 생성할 때, 이전에 생성된 블록의 해시값이 새로운 블록의 헤더에 포함된다. 해시값을 입력으로 해서 원래의 값인 이전 블록을 알아내기가 현실적으로 불가능하기 때문에, 블록의 내용을 위변조하는 것이 불가능하다. Fig. 1은 블록체인의 일반적인 구조를 나타낸다.

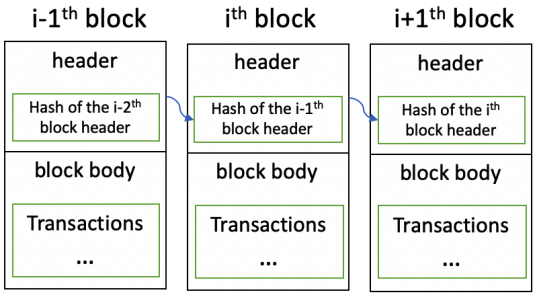

Fig. 1. Logical representation of a blockchain

2.2 블록체인의 종류

블록체인의 응용과 블록체인 네트워크로의 참여 방식에 따라서 블록체인을 다음과 같이 구분할 수 있다. 제3자의 허가나 승인없이 참여자가 자유롭게 블록체인 네트워크에 참여하고 탈퇴할 수 있는 블록체인을 퍼블릭 블록체인이라고 한다. 자발적으로 퍼블릭 블록체인으로 참여를 유도하기 위해서 블록 채굴에 성공한 참여자에게는 인센티브가 주어진다. 프라이빗 블록체인은 특별한 목적을 위해서 개인 또는 기관이 만든 것으로 관리자에 의해서 허용된 참여자만이 블록을 생성할 수 있다. 컨소시움 블록체인은 여러 기관이 공동의 목적으로 만든 블록체인으로서 프라이빗 블록체인과 마찬가지로 사전에 허용된 경우에만 참여를 할 수 있다.

이처럼 블록체인을 참여 허용 여부에 따라서 허가형 블록체인과 비허가형 블록체인으로도 구분할 수 있다. 일반적으로 퍼블릭 블록체인은 비허가형 블록체인이며, 프라이빗 블록체인과 컨소시움 블록체인은 허가형 블록체인으로 볼 수 있다. 한편, 사물인터넷의 경우에는 사용자가 아닌 사물도 블록체인 네트워크에 참여할 수 있기 때문에 그러한 구분이 명확하지 않을 수 있다. 즉, 퍼블릭과 프라이빗은 구분은 블록체인 접근에 대한 인증에 관한 문제이고, 허가형과 비허가형은 사물인터넷 기기가 할 수 있는 일에 대한 권한 부여의 문제로 볼 수 있다[3].

2.3 합의 알고리즘

블록체인의 합의 알고리즘은 참여자가 채굴한(즉, 생성한) 블록을 어떻게 승인하는가에 관한 것이다. 비트코인의 경우는 이전 블록이 생성된 이후에 가장 먼저 채굴된 블록이 우선적으로 승인된다. 우선적이란 말은, 그보다 늦게 채굴된 블록이 있을 경우에, 그 블록을 이어서(즉, 그 블록을 기반으로 생성된 해시값을 포함한) 다음 블록을 더 빠르게 생성한다면(6개 이상 블록이 이어진 경우) 나중에 채굴된 블록이 최종적으로 승인되며, 그보다 먼저 생성된 블록은 승인 취소가 된다[11]. 승인이라는 것도 특정인이 부여하는 것이 아니라, 블록체인 네트워크에 참여한 사용자들이 막 채굴된 블록을 기반으로 그 이후에 블록들을 생성하게 된다면 자동적으로 채굴된 이 블록을 '승인'되었다고 볼 수 있다.

누구나 블록을 생성할 수 있지만 아무나 블록을 생성하지 못하도록, 채굴자가 그 블록을 채굴하기 위해서 특정한 노력을 들였다는 것을 증명해야 그 블록을 채굴했다고 인정해준다. 이를 작업 증명(Proof of Work, PoW)이라고 한다. 작업 증명은 해시함수의 입력으로 무차별 대입을 한 결과가 특정값보다 작게 나온 경우(이를 '난스(nonce)'라고 함)에 완료가 된다[2]. 이 과정에서 엄청난 컴퓨팅 자원이 소비가 되므로, 컴퓨팅 능력이 부족한 경량의 사물인터넷 기기들은 작업 증명을 수행하기가 매우 어렵다[2,8].

작업 증명 기반의 합의 알고리즘은 채굴을 위해서 과도한 컴퓨팅 자원 및 에너지가 소비되며, 가장 먼저 블록을 채굴한 채굴자에게만 보상이 주어지므로 채굴의 독점화가 발생한다. 이러한 문제점을 해결하기 위해서 참여자의 소유 지분(stake)이 블록 생성 권한에 반영되는 지분 증명(Proof of Stake, PoS)이 개발되었다. 지분 증명에서는 채굴자라는 용어 대신에 검증자(validator)라는 용어를 사용한다. 참여자들이 보유한 지분의 비율에 따라서 검증자가 선택되고 이 검증자가 블록을 검증하여 최종적으로 블록체인에 포함시킨다. 가장 많은 지분을 가진 검

2) 원래는 정확한 원래의 값을 찾아야 하지만 현실적으로 불가능하기 때문에 특정값보다 작게 나와도 인정이 되며, 이 값을 조절함으로써 난이도를 조절할 수 있다. 비트코인의 경우 10분에 하나의 블록을 채굴할 수 있도록 설계되었으며, 참여자가 많거나 참여자들의 컴퓨팅 파워가 높아 10분 이내에 채굴이 가능하다면 난이도를 높이며(즉, 목표값을 낮추어), 난이도가 너무 높아 블록을 채굴하는데 10분 이상이 소요되면 난이도를 낮춘다. 컴퓨팅 성능이 낮은 사물인터넷 기기를 이용해서 작업 증명을 수행한다면 난이도를 낮출 필요가 있다.

증자만이 선택되는 것을 방지하기 위해서 무작위 블록 선택이나 코인 나이에 따른 선택 등이 추가적으로 사용된다. 해시값을 찾는 과정이 없기 때문에 과도한 컴퓨팅 자원을 소비하지 않는다는 장점이 있으나, Nothing at Stake 문제가 발생할 수 있다는 단점이 있다[2]. 이는 동시에 두 블록이 생성되어서 어떤 블록이 진짜인지를 가릴 때, 참여자는 지분에 따라서 투표하기 때문에 두 곳에 투표를 해도 손해를 보지 않기 때문에 결국 합의에 이르기 어렵게 될 수 있다.

위임 지분 증명(Delegated Proof of Stake, DPoS)은 암호화폐 소유자들이 각자의 지분율에 비례하여 투표를 하여 대표자를 선정하고, 이 대표자들끼리 합의하여 의사결정을 내리는 합의 알고리즘이다. 합의를 수행하는 노드의 수가 PoW나 PoS보다 적기 때문에 보다 빠르게 블록을 생성할 수 있다. 다만, 많은 지분을 가진 참여자가 투표권을 남용하여 자신에게 유리한 대표자를 선출할 수가 있어 중앙 집중화 및 투명성에 우려가 있다.

앞서 살펴본 합의 알고리즘은 제 3자에 의한 허가 없이도 누구나 블록체인 네트워크에 참여하는 퍼블릭 블록체인에 사용된다. PBFT(Practical Byzantine Fault Tolerance)은 네트워크에 참여한 모든 사람들을 서로 알고 있는 프라이빗이나 컨소시움 블록체인에 활용될 수 있는 합의 알고리즘이다. 참여자 중에서 선출된 리더는 자신을 포함한 모든 참여자에게 합의 요청을 보내고, 그 요청에 대한 결과를 집계하여 2/3 표를 획득하면 블록을 생성한다. 일부 비정상적인 참여자가 있더라도 정상 작동되며, 이때 부정한 참여자의 수를 n이라고 한다면 총 참여자의 수는 3n+1 이상이어야 한다. 합의를 이루어가는 과정에서 참여자들 간에 합의 요청을 위한 메시지를 발생하기 때문에 참여자의 수가 많아질수록 통신에 대한 부담이 커진다는 단점이 있다. Table 1은 블록체인에 적용되는 대표적인 합의 알고리즘을 비교한다[10].

3. 블록체인-사물인터넷 선행 연구

클라우드 컴퓨팅 기술 기반의 현재의 사물인터넷 구조는 복잡한 대규모 데이터를 신속하게 처리하기에는 효율적이지만, 다음과 같은 한계를 지니고 있다[2]. 중앙 집중형으로 인해 장애 발생 시 여러 부분에 큰 영향을 미칠 수 있으며, 개인정보의 유출 가능성이 있고, 클라우드 상에서 데이터 추적 및 관리에 어려움을 겪을 수 있다. 또한, 네트워크 말단에 위치한 사물인터넷 기기로부터 입력된 데이터를 클라우드를 통해서 처리하고 응답 받기까지 종단간 지연 시간이 증가될 수 있다.

이러한 한계를 극복하기 위해서 최근에 분산 원장 기술 기반의 블록체인을 사물인터넷에 접목하려는 연구가 많이 진행되었다[2,3,6,10,21]. 블록체인-사물인터넷 결합을 통해서 얻을 수 있는 이점은 다음과 같다[2,6]. P2P 네트워크 기반으로 탈중앙화가 가능해짐으로써 단일 장애 지점을 제거하게 되어 장애 발생 시 문제를 최소화할 수 있으며, 중앙 서버로의 병목 문제 해결, 제 3자 관리 제거, 데이터 위변조 방지 및 관리 책임성 제공, 스마트 컨트랙트를 이용한 프로그램이 가능한 로직 제공, 접속 제어 및 인증 제공 등이 가능해진다. 한편, 센서 등과 같이 말단의 사물인터넷 기기들은 블록의 검증 및 채굴을 수행하기에 컴퓨팅 성능이 부족한 경우가 있어 게이트웨이를 활용하거나[10,12,13], 다계층 구조[7,9], 또는 에지 컴퓨팅 기술[3,8] 등을 이용하려는 노력이 있어 왔다. 본 절에서는 사물인터넷에 블록체인을 적용하기 위한 선행 연구들을 분석한다.

블록체인을 사물인터넷에 적용하기 위해서는 사용자 단말에서부터 모든 네트워크 기기에 블록체인 관련 기능이 제공되어야 한다. Cha 등은 사물인터넷 서비스 제공자가 사물인터넷 기기를 수정 또는 교체하지 않고도 개인정보 유출을 방지할 수 있는 게이트웨이 기반의 블록체인 기술을 제안하였다[12]. 블록체인 게이트웨이는 블

Table 1. Comparison of consensus algorithms for blockchain

items	PoW	PoS	DPoS	PBFT
blockchain type	public	public	public	private, consortium
trust among peers	non-turst	non-trust	non-trust	trust
decentralized level	decentralized	decentralized	centralized	centralized
energy/resource consumption	high	lower than PoW	low	low
processing speed (transactions/sec)	around seven (Bit coin)	several hundreds	several thousands	several thousands
security level	high	high	low	low
applications	Bitcoin	Qtum	EOS	Hyperledger Fabric

록체인 네트워크의 계정을 기반으로 사용자 및 사용자 기본 설정을 식별한다. 관리자는 게이트웨이에 사물인터넷 기기 정보 및 프라이버시 정책 등을 등록하기 위해서 스마트컨트랙트를 생성한다. 사용자는 게이트웨이를 통해서 사물인터넷 기기에 접속을 하고, 게이트웨이는 저장된 사용자 설정 정보에 기반해서 사용자 요구를 처리한다.

사물인터넷의 통신 기술 중에서 저전력으로 광대역을 구현하려는 LPWAN(low power wide-area-network)에서도 블록체인 기술을 적용하려는 시도가 있다. LPWAN은 비면허 대역을 기반으로 하는 LoRaWAN(long range WAN)과 셀룰러 통신망을 이용하는 NB(narrow band)-IoT 등이 있다. 이 중에서 LoRaWAN은 비면허 대역을 이용하여 개인 또는 조직이 구현 및 운영하므로 사용자와 관리자 간의 신뢰성 및 관리 문제가 발생할 수 있기 때문에, Lin 등은 이를 블록체인으로 해결하고자 한다[13]. 네트워크는 센서 데이터 수집/전송, 외부 시스템 제어 및 MCU로 동작하는 LoRa 트랜시버를 탑재한 단말, TCIP/IP를 이용해서 단말로부터의 데이터를 네트워크 서버로 전달(브리지 역할)하는 게이트웨이, 데이터 처리/저장, 단말의 출력 제어 등을 수행하는 네트워크 서버 등으로 구성된다. 다른 선행 연구에서는 게이트웨이가 블록체인의 기능을 일부 수행하는데 반해서[10,12], 이 연구에서는 블록체인은 네트워크 서버에서 동작된다. 다만, 논문에서는 LoRaWAN에 특화된 블록체인 동작 방식 및 구현에 대한 자세한 결과는 제시되지 않아 향후 후속 연구가 필요해 보인다.

사물인터넷을 구성하는 기기들은 컴퓨팅 성능, 저장공간, 전력공급, 네트워킹 능력, 이동성 등에 있어서 다양한 성능 규격을 갖는다. 따라서 블록체인 기술을 적용하는데 있어서도 성능과 응용에 따라서 다르게 구현될 수 밖에는 없다. IBM은 확장성 및 보안이 강화된 블록체인-사물인터넷 개념 증명을 위해서 3가지 피어 구조를 제시하였다[9]. Light peer는 가벼운 응용을 지원하는 작은 센서, 기기 등과 같이 낮은 메모리 및 저장공간을 갖춘 기기들에 적용될 수 있는 구조이다. 블록체인을 저장하지 않으며, 블록체인 주소 및 잔고를 저장하는 가벼운 지갑(light wallet)을 관리한다. 자신과 관련된 블록체인 내의 트랜잭션을 얻기 위해서는 light peer는 다른 신뢰할 수 있는 피어를 의지한다. Standard peer는 핵심 프로토콜은 light peer와 유사하나, 일정 기간 동안 블록체인의 일부를 보유할 수 있다. 이는 자신의 최근 트랜잭션이나 계약상의 합의일 수 있다. Standard peer는 light peer의 파일 교환을 지원하며 피어들 간에 메시지 교환을 수행한다. Peer Exchange는 높은 처리 능력 및 저장 공간을 갖춘 고성능 기기로서, 조직이나 기관이 운용하는 피어이다. 블록체인 전체를 저장하고 복합한 질의 및 블록체인 분석 등의 기능을 수행하게 된다.

Dorri 등도 사물인터넷 기기의 성능 제약을 고려하여 계층적인 블록체인 기반 사물인터넷 구조를 제시하고 있다[7]. 로컬 프라이빗 블록체인을 운용하는 스마트홈, 클라우드 스토리지, 그리고 오버레이 네트워크로 구성되는 3-티어 구조를 갖는다. 스마트홈은 온도계, 전구, 카메라 및 각종 센서들과 같은 스마트 기기, 로컬 저장공간, 그리고 스마트 기기들이 발생시킨 트랜잭션들을 처리하는 사설 로컬 블록체인으로 구성된다. 오버레이 네트워크는 블록체인의 P2P 네트워크와 유사하며, 스마트홈 채굴자, 스마트홈의 고성능 장치, 사용자 단말 등이 노드로서 구성된다. 네트워크 오버헤드 및 지연 감소를 위해서 노드들은 클러스터로 묶인다. 개별 클러스터는 클러스터 헤드를 선출하고, 클러스터 헤드들은 퍼블릭 블록체인을 운영한다.

블록체인을 사물인터넷에 적용하는데 있어서 해결해야 할 이슈 중의 하나는 각종 기기에서 발생하는 데이터들을 신속하게 처리하는 것이다. 사물의 수가 증가할수록 이에 대한 부담도 같이 증가하기 때문에, 클라우드 컴퓨팅이 감당하기 어렵게 되므로 에지 컴퓨팅 기술[3]을 이용하여 분산 처리할 필요가 있다[8]. 에지 컴퓨팅은 여러 지역에서 물리적으로 분산되어 사물로부터의 데이터 송수신시 저지연 처리가 가능하며, 트래픽 분산 및 부하 분산에 유리하다[3,4]. Fernández-Caramés 등은 단일 보드 컴퓨터로 구현된 포그 컴퓨팅이 로컬 게이트웨이로 동작하여 사물인터넷 기기의 요청에 빠르게 응답할 수 있는 구조를 제시하고 있다[3]. 사물인터넷 기기들은 포그 컴퓨팅이 있는 포그 계층을 거쳐서 클라우드로 연결될 수 있다. 또 다른 가능한 구조로서, 고성능 서버로 구성되어 경량의 클라우드 컴퓨팅 기능을 수행하는 클라우드릿(Cloudlet)이 포함된 에지 컴퓨팅 계층을 제시한다. 이는 포그 계층과 유사하나, 블록체인의 풀노드(full node)와 같이 보다 복잡한 성능을 요구하는 사물인터넷 기기에 보다 신속하게 응답할 수 있다.

사물인터넷 기기나 이동 단말들은 일반적으로 컴퓨팅

3) 에지 컴퓨팅(edge computing)은 중앙형인 클라우드 컴퓨팅에 비해서 사용자 단말에 보다 가깝게 위치한 컴퓨팅 자원이라는 의미로 '에지' 라고 표현된다[4]. 에지 컴퓨팅의 실현으로 포그 컴퓨팅(fog computing), 모바일 에지 컴퓨팅(mobile edge computing), 클라우드릿(cloudlet) 등이 있다. 이와 관련해서는 4장에서 보다 상세히 설명한다.

자원이 부족한 경우가 많아 블록 채굴이나 합의 과정을 수행하기에 제약이 있다. 이를 극복하기 위해서 모바일 에지 컴퓨팅 기술을 활용하려는 연구가 진행되었다[8]. 모바일 에지 컴퓨팅은 무선 접속망에서 기지국에 서버를 두어 작은 데이터센터를 구축함으로써 클라우드 컴퓨팅 서비스를 모바일 네트워크의 에지에서 제공한다[14]. 사용자(즉, 사물인터넷 기기나 이동 단말)들은 블록체인 애플리케이션을 동작시키며, 블록 채굴은 모바일 에지 컴퓨팅으로부터 컴퓨팅 자원을 빌려서 수행한다. 즉, 모바일 에지 컴퓨팅이 채굴자로서 동작을 하게 된다. 여러 사용자들이 동시에 모바일 에지 컴퓨팅 자원을 요청할 수 있기 때문에 효율적인 자원 분배 및 할당 기술이 필요하다[15].

4. 에지 컴퓨팅 기반의 사물인터넷을 위한 블록체인 적용 방안

앞 장에서는 사물인터넷에 블록체인 기술을 적용할 때 얻게 되는 장점과 이러한 장점을 얻기 위해서 선행되었던 블록체인-사물인터넷 결합 기술에 대해서 살펴보았다. 다방면으로 연구가 진행되었는데, 특히 컴퓨팅 자원 부족으로 인해 사물인터넷 기기가 직접 블록 생성에 참여하기 어려운 점을 해결함이 중요함을 알 수 있었다. 사물인터넷 구조에서 사물인터넷 기기와 클라우드의 중간 계층으로 저장공간 및 처리 능력을 제공할 수 있는 에지 컴퓨팅 기술을 활용한다면, 센서나 아두이노와 같은 컴퓨팅 자원이 부족한 사물인터넷 기기들도 블록체인 네트워크에 참여할 수 있게 되며, 신속한 트랜잭션 처리 및 블록 생성이 가능하게 된다. 본 장에서는 에지 컴퓨팅 기반의 사물인터넷에 블록체인 기술을 적용하기 위한 방안을 소개한다.

4.1 에지 컴퓨팅 기반의 사물인터넷- 블록체인 결합 구조

1) 에지 컴퓨팅 기술

Bilal 등에 따르면 에지 컴퓨팅(edge computing) 기술은 "네트워크의 가장자리에서 지연을 최소화하면서 실시간으로 컴퓨팅 자원 및 저장공간을 제공하는 여러 신기술들을 아우르는 기술"로 정의하고 있다[4]. 에지 컴퓨팅은 에지 노드의 역할 및 성능, 노드의 위치, 네트워크, 제공하는 서비스 등에 따라서 몇 가지로 구분될 수 있다. 포그 컴퓨팅(fog computing)은 사용자 근처에서 클라우드 컴퓨팅 서비스를 제공하기 위해서 시스코 사에서 처음 제안하였다[16]. 말단 기기와 전통적인 클라우드 컴퓨팅 데이터센터 사이에서 컴퓨팅 자원, 저장 공간, 네트워킹 서비스를 제공하는 고도화된 가상 플랫폼을 의미한다. 중앙형인 클라우드 컴퓨터와는 달리 포그 컴퓨팅은 사용자에 가깝게 분산 배치되며 특정 지역을 커버하기 때문에 사용자의 요구를 보다 신속히 처리할 수 있다. 포그 컴퓨팅은 사용자 단말-포그-클라우드의 3계층을 구성되는데, 포그 노드는 단말로부터의 데이터를 클라우드로 전달하지 않고 로컬에서 저장 및 처리를 할 수 있다. 포그 컴퓨팅을 구성하는 포그 노드는 셋탑박스, 게이트웨이, 액세스 포인트, 라우터, 스위치, 차량, 사용자 단말 등이 될 수 있다. 포그 컴퓨팅은 사물인터넷을 지원하기 위한 플랫폼으로 고안되었으며, 동시에 여러 사용자들로부터의 서비스 요청을 받게 될 경우 자원 관리 및 부하 분산을 적절히 처리할 수 있어야 한다.

모바일 에지 컴퓨팅 기술(Mobile edge computing, MEC)은 모바일 네트워크의 가장자리에서 IT 서비스 환경과 클라우드 컴퓨팅 기능을 제공하기 위해서 ETSI가 제안하였다[17]. 모바일 에지 컴퓨팅도 클라우드와 이동단말 사이에 MEC가 존재하는 3계층 구조를 가지며, 사용자로부터의 트래픽은 중앙의 클라우드로 전송하는 대신에 MEC 서버로 전달되어 처리된다. MEC 서버는 LTE 매크로 기지국(eNodeB)나 3G 무선 네트워크 제어기(RNC) 등에 위치할 수 있다. 모바일 에지 컴퓨팅은 이동통신 사업자가 주도적으로 운영한다.

클라우드릿(Cloudlet)은 클라우드 서비스를 이동 사용자에게 좀 더 가깝게 제공할 목적으로 카네기멜론대학에서 제안하였다[18]. 고성능의 멀티코어 컴퓨터들을 클러스터로 구성하여 작은 데이터센터('data center in a box' 개념)로 운영하며, 사용자와 가까운 거리에 위치함으로써 사용자 단말의 처리 부담을 클라우드릿으로 전가할 수 있게 한다. 클라우드릿도 이동단말-클라우드릿-클라우드로 구성되는 3계층 구조를 가지며, 사용자는 원거리에 있는 클라우드 대신에 근거리에 있는 클라우드릿으로부터 컴퓨팅 자원을 보다 빠르게 사용할 수 있다. 클라우드릿은 WiFi AP나 LTE 기지국 등에 배치될 수 있으며, 병원, 쇼핑센터, 사무실 등 사업장 인근에 위치하게 된다. 사용자들은 원거리에 있는 중앙 클라우드에 접속하지 않고도 지연을 최소화하면서 높은 컴퓨팅 자원을 사용하기 위해서 적절한 에지 컴퓨팅 기술들을 사용할 수 있다. Table 2는 앞서 살펴본 에지 컴퓨팅 기술들을 비교한다[4,5,19].

Table 2. Comparison of edge computing technologies

feature	fog computing	mobile edge computing	cloudlet
node equipment	router, switch, AP, gateway	servers in base stations	high performance computing servers
node location	between IoT devices and cloud	Radio Network Controller, base station	inside building (office, shopping center, etc)
distance from users	one hop or more	one hop	one hop
provided services	computing resource storage, networking	computing resource, storage	cloud computing
access methods	Wi-Fi, mobile networks	mobile networks	Wi-Fi
operator	IoT service provider	mobile network operators	datacenter provider

2) 에지 컴퓨팅 기반 사물인터넷-블록체인 결합 구조

본 논문은 사물인터넷 기기 계층, 에지 컴퓨팅 계층, 클라우드 컴퓨팅 계층의 3계층으로 구성된 에지 컴퓨팅 기반의 사물인터넷 구조를 Fig. 2와 같이 제시한다. 사물인터넷 기기 계층에는 스마트폰, 가전기기, TV, 자동차, 각종 센서 등이 존재한다. 사물인터넷 기기들은 센싱 데이터를 포함한 여러 트랜잭션들을 발생시킨다. 기기의 성능 및 응용에 따라서 DApp이 탑재되거나 전자지갑을 보유할 수 있다. 사물인터넷 기기 계층에는 사물인터넷 기기와 상위에 있는 에지 컴퓨팅 계층의 기기와의 중계 역할을 해주는 사물인터넷 게이트웨이가 존재한다. 사물인터넷 기기에 따라서 에지 컴퓨팅 장치로 직접 연결되거나 게이트웨이를 거칠 수도 있다. 에지 컴퓨팅 계층에는 포그 컴퓨팅, 모바일 에지 컴퓨팅, 그리고 클라우드릿 등이 존재할 수 있다. 앞서 살펴본 바와 같이 포그 컴퓨팅 장치는 주로 사물인터넷 사업자가 운영하고, 모바일 에지 컴퓨팅 장치는 이동 통신 사업자가, 그리고 클라우드릿 장치는 데이터센터 사업자가 주로 운영을 한다. 제한된 컴퓨팅 성능을 가진 사물인터넷 기기가 고수준의 컴퓨팅 처리를 해야 하는 경우에는 에지 컴퓨팅으로부터 자원을 요청하여 이를 처리할 수 있다. 에지 컴퓨팅 장치로도 자원 부족으로 처리가 어려운 경우에는 에지 컴퓨팅 장치는 상위의 클라우드 컴퓨팅 장치와 연결되어 고수준의 컴퓨팅 처리를 요청할 수 있다.

4.2 에지 컴퓨팅 기반의 사물인터넷 에서의 블록체인 동작

본 논문에서 제안한 3계층으로 구성된 에지 컴퓨팅 기반의 사물인터넷 구조에서 블록체인의 동작 과정을 Fig. 3에서 제시한다. 사물인터넷 기기들은 트랜잭션 생산자가 되며, 사물인터넷 게이트웨이와 에지 컴퓨팅 장치들은 트랜잭션의 유효성 검증 및 블록을 생성하는 피어로 동작한다. 사물인터넷 기기들이 트랜잭션을 생산하면 이를 블록으로 생성하기 위해서 사물인터넷 게이트웨이로 전달한다. 게이트웨이는 수신한 트랜잭션의 유효성을 검증한다. 만약에 게이트웨이가 블록 채굴을 위한 충분한 컴

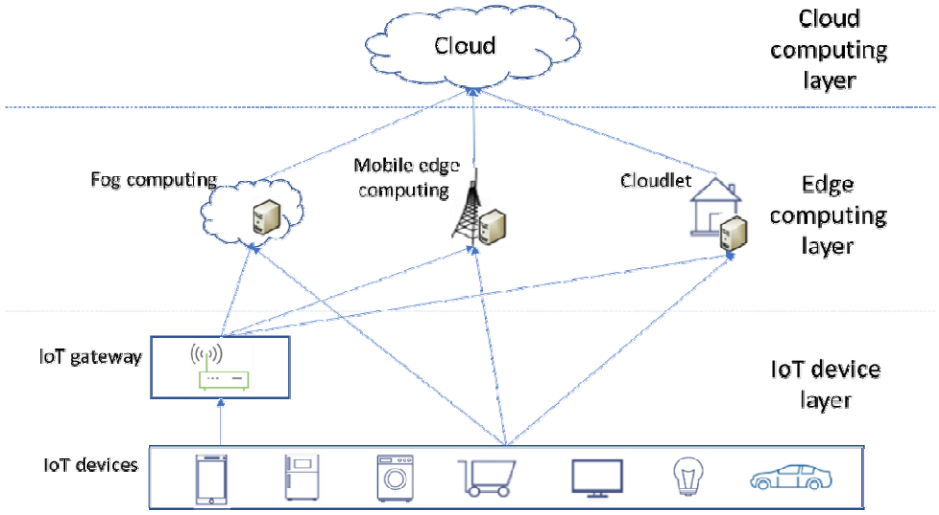

Fig. 2. Edge computing-based Internet of Things architecture applied for Blockchain

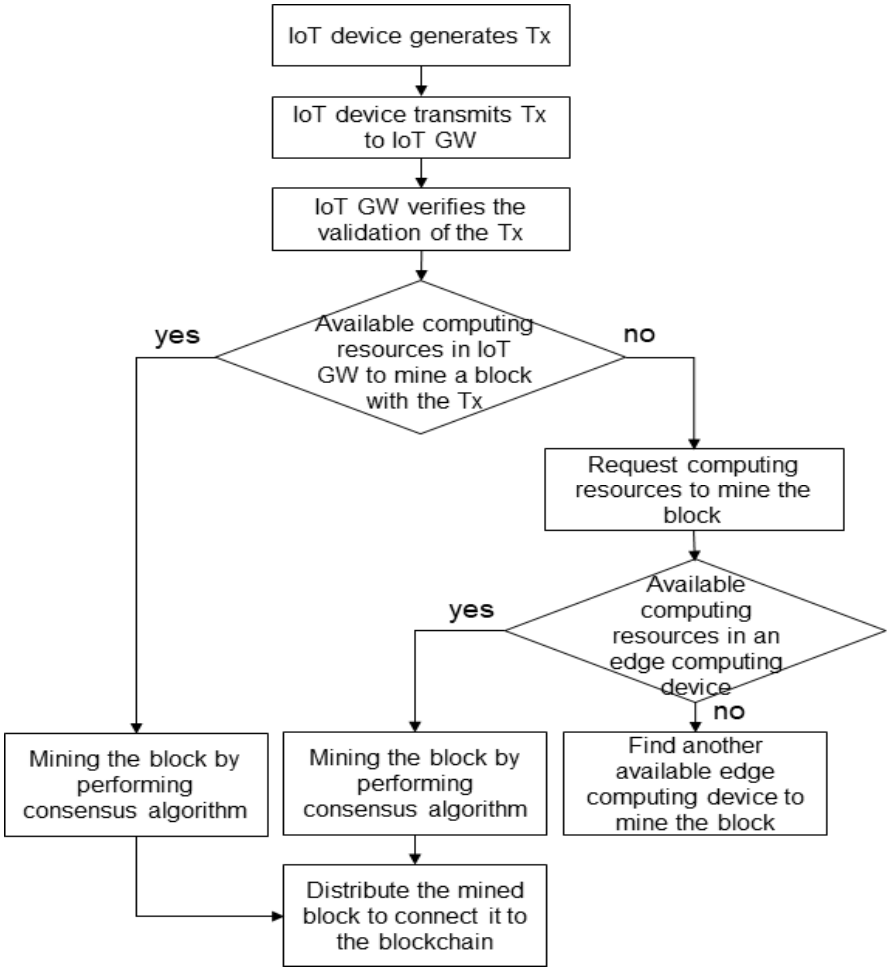

Fig. 3. Operational procedure of blockchain in edge computing-based Internet of Things

퓨팅 자원이 있다면 합의 알고리즘을 수행하여 블록을 채굴하고, 이를 블록체인 네트워크에 배포함으로써 해당 블록에 블록체인에 연결되도록 한다. 만약에 해당 게이트웨이가 충분한 컴퓨팅 자원을 가지지 못했다면, 에지 컴퓨팅 장치에 블록을 채굴할 수 있도록 컴퓨팅 자원의 임대를 요청한다. 충분한 컴퓨팅 자원을 가진 에지 컴퓨팅 장치는 블록 채굴을 위한 합의 알고리즘을 수행하고, 채굴한 블록을 블록체인 네트워크에 배포하여 최종적으로 블록체인을 생성한다. 특정 지역에 있는 에지 컴퓨팅 장치에 블록 채굴을 위해서 동시에 자원 요청이 몰리게 되면 해당 장치에 컴퓨팅 자원이 부족하게 될 수도 있다. 이러한 경우에는 게이트웨이는 다른 가용한 에지 컴퓨팅 장치에게 컴퓨팅 자원을 요청하게 된다. 따라서 블록 채굴을 위한 자원 요청에 따른 에지 컴퓨팅 장치들 간의 자원의 효율적인 관리 방안이 필요하다. 만약, 인근에 가용한 자원이 있는 에지 컴퓨팅 장치가 없다면 중앙의 클라우드 컴퓨팅 장치에 자원을 이용할 수도 있다. 합의 알고리즘에 의해서 블록이 채굴되면, 채굴된 블록은 블록체인 네트워크로 배포되어 최종적으로 블록체인에 연결된다. 백업용으로 블록체인이 클라우드 컴퓨팅 장치에 저장될 수 있다.

에지 컴퓨팅을 활용하여 블록체인을 운용하는 과정에 있어서, 컴퓨팅 자원 이용을 통한 블록 채굴에 따른 보상과 에지 컴퓨팅 서비스 제공에 따른 비용 간의 상충을 만족시킬 필요가 있다[15]. 또한 블록 채굴을 위해서 가용한 에지 컴퓨팅 장치가 다수 존재할 경우에, 전송 지연과 네트워크 자원 소비를 고려하여 최적의 에지 컴퓨팅 장치 선택 알고리즘이 요구된다.

5. 결론

본 논문은 에지 컴퓨팅 기술이 도입된 사물인터넷 구조에서 블록체인을 적용하기 위한 방안을 연구하였다. 탈중앙화 방식의 블록체인 기술을 사물인터넷에 적용함으로써 단일 장애 지점 해소를 통해 장애에 강인해지고, 중앙 서버로의 병목 문제가 해소되며, 통신 중인 데이터의 무결성을 보장하는 등 여러 측면에서의 잇점을 얻을 수 있다. 하지만 블록을 채굴하는 과정에서 막대한 컴퓨팅 자원이 소비될 수 있으므로 자원이 부족한 사물인터넷 기기가 직접 블록체인 네트워크에 참여하기 어려울 수 있다. 이를 해소하기 위해서 사물인터넷 기기가 접속하는 네트워크의 가장자리에 배치되는 에지 컴퓨팅 장치로부터 컴퓨팅 자원을 임대하여 블록 채굴을 할 수 있다.

향후 에지 컴퓨팅 기반의 사물인터넷에서 블록체인 기술을 개발하기 위해서 추가로 진행되어야 할 연구 과제는 다음과 같다. 특정 지역을 담당하는 에지 컴퓨팅 장치가 다수로부터 자원 요청을 받을 경우 가용한 자원이 부족해 질 수 있는 가능성이 존재하므로, 블록체인 참여자의 요청에 따른 에지 컴퓨팅 장치의 효율적인 관리에 대한 연구가 필요하다. 특히, 컴퓨팅 자원 이용을 통한 블록 채굴에 따른 보상과 에지 컴퓨팅 서비스 제공에 따른 이익 간의 상충을 만족시킬 필요가 있다. 다음으로, 사물인터넷 기기가 참여한 블록체인 네트워크 사업자와 에지 컴퓨팅 서비스 사업자가 상이한 경우에 컴퓨팅 자원 서비스 요청에 대한 연동 방안이 요구된다. 또한 자원 임대에 따른 비용 정산에 대한 방안이 필요하다. 일반적인 블록체인 네트워크에 비해서 사물인터넷은 엄청나게 많은 기기들이 연결되기 때문에 무엇보다도 확장성이 요구된다. 이를 위해서 블록이 하나의 체인으로 연결된 구조를 탈피해서, 하나의 블록이 여러 선행 블록과 연결되는 blockDAG 이나 블록이 아닌 트랜잭션으로 구성되는 TDAG와 같은 블록리스 구조에 대한 심도있는 연구가 필요하다.

REFERENCES

[1] Cisco, V. N. I. (2018). Cisco visual networking index: Forecast and trends, 2017-2022. *White Paper, 1.*

[2] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21(2),* 1676-1717.

[3] Fernández-Caramés, T. M. & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access, 6,* 32979-33001.

[4] Bilal, K., Khalid, O., Erbad, A. & Khan, S. U. (2018). Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers. *Computer Networks, 130,* 94-120.

[5] Dolui, K. & Datta, S. K. (2017, June). Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

[6] Reyna, A., Martín, C., Chen, J., Soler, E. & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88,* 173-190.

[7] Dorri, A., Kanhere, S. S. & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187.*

[8] Xiong, Z., Zhang, Y., Niyato, D., Wang, P. & Han, Z. (2018). When mobile blockchain meets edge computing. *IEEE Communications Magazine, 56(8),* 33-39.

[9] Panikkar, S., Nair, S., Brody, P. & Pureswaran, V. (2015). Adept: An iot practitioner perspective. *Draft Copy for Advance Review, IBM.*

[10] Makhdoom, I., Abolhasan, M., Abbas, H. & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications, 125,* 251-279.

[11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[12] Cha, S. C., Chen, J. F., Su, C. & Yeh, K. H. (2018). A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access, 6,* 24639-24649.

[13] Lin, J., Shen, Z. & Miao, C. (2017, July). Using blockchain technology to build trust in sharing LoRaWAN IoT. In *Proceedings of the 2nd International Conference on Crowd Science and Engineering* (pp. 38-43). ACM.

[14] Abbas, N., Zhang, Y., Taherkordi, A. & Skeie, T. (2017). Mobile edge computing: A survey. *IEEE Internet of Things Journal, 5(1),* 450-465.

[15] Xiong, Z., Feng, S., Niyato, D., Wang, P. & Han, Z. (2017). Edge computing resource management and pricing for mobile blockchain. *arXiv preprint arXiv:1710.01567.*

[16] Bonomi, F., Milito, R., Zhu, J. & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). ACM.

[17] Hu, Y. C., Patel, M., Sabella, D., Sprecher, N. & Young,

V. (2015). Mobile edge computing—A key technology towards 5G. *ETSI white paper, 11(11),* 1-16.

[18] Satyanarayanan, M., Bahl, V., Caceres, R. & Davies, N. (2009). The case for vm-based cloudlets in mobile computing. *IEEE pervasive Computing*.

[19] Wang, S., Zhang, X., Zhang, Y., Wang, L., Yang, J. & Wang, W. (2017). A survey on mobile edge networks: Convergence of computing, caching and communications. *IEEE Access, 5,* 6757-6779.

[20] Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J. & Ko. K. (2017). Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access, 6,* 1513-1524.

[21] S. Hong & S. Park. (2017). The Research on Blockchain-based IoT Authentication. *Journal of the Korea Convergence Society, 8(11),* 57-62.

최 정 열(Jung-Yul Choi) [정회원]

· 2000년 2월 : 인하대학교 전자공학과 (공학사)
· 2006년 8월 : 한국정보통신대학교 공학부(공학박사)
· 2006년 9월 ~ 2011년 2월 : (주) KT 선임연구원
· 2011년 3월 ~ 현재 : 성결대학교 컴퓨터공학부 부교수
· 관심분야 : 사물인터넷, 에지 컴퓨팅, 블록체인, 머신러닝, 그린 통신망,
· E-Mail : passjay@gmail.com