논문 20-45-08-07 The Journal of Korean Institute of Communications and Information Sciences '20-08 Vol.45 No.08
https://doi.org/10.7840/kics.2020.45.8.1373

블록체인 기반 차량 컨텐츠 결제 프로토콜

김 우 성◆

Vehicular Content Payment Protocol Using Blockchain

Wooseong Kim◆

요 약

미래 자동차 기술은 단순한 이동 목적을 떠나 컴퓨팅 환경으로써의 다양한 역할을 할 것으로 예측된다. 현재에도 테슬라 전기 자동차에서 승객을 위한 지능형 서비스를 제공하고 있으며, 자율 주행 기능 또한 발전하고 있다. 이러한 자동차들은 각 종 센서를 통한 주행 및 교통 정보 수집 뿐만 아니라, 다양한 인포테인먼트 혹은 차량간 컴퓨팅 자원 공유를 위한 다양한 활동이 요구된다. 이에 5G 이동 통신에서는 차량간 통신 환경을 제공하고 있으며, 차량 안전 데이터와 사용자 데이터 전송을 가능하게 한다. 이러한 차량 포그 컴퓨팅 환경에서 유통되는 데이터와 컨텐츠에 대한 보안 및 신뢰성 보장은 차량 안전을 위해 매우 중요하다. 최근 이러한 목적에 부합하는 P2P 네트워크 기반 분산 원장으로 블록체인 기술이 사용되고 있다. 더불어 블록체인에 기반한 결제 채널 네트워크 프로토콜은 사용자로 하여금 직접 거래를 가능하게 하고 기존 블록체인이 가지고 있는 확장성 문제를 해결하는 주요 기술로 떠오르고 있다. 본 논문에서는 차량 포그 내에서 차량간 컨텐츠 거래를 위해 결제 채널 프로토콜을 제안하고 구현하였다. 이를 기반으로 테트스 베드 구축 하고 실험을 통해 실현 가능성을 입증하였다.

Key Words : communication, signal processing, Neutral systems, Communication Sciences, Network, Blockchain, Payment channel network, Vehicular cloud

ABSTRACT

Start after striking space key 2 times. It is predicted that future automobile technology will play a variety of roles as a computing environment, not just for the purpose of moving. Even today, Tesla electric vehicles provide intelligent services for passengers, and self-driving functions. These vehicles require various activities to collect driving and traffic information through various sensors, as well as to share various infotainment or computing resources between vehicles. Accordingly, 5G mobile communication provides an inter-vehicle communication environment, and enables vehicle safety data and user data transmission. Security and reliability of data and contents distributed in the vehicle fog computing environment are very important for vehicle safety. Blockchain technology has been recently used as a distributed ledger based on P2P networks that meets these goals. In addition, the blockchain-based payment channel network is emerging as a major technology that enables users to directly trade and solves the scalability problems of existing blockchains. In this paper, a payment channel protocol was proposed and implemented for content transaction between vehicles in a vehicular fog. Based on this, the testbed was built and the feasibility was proved through experiments.

◆ First Author : Gachon University Department of Compute engineering, wooseong@gachon.ac.kr, 부교수, 정회원
논문번호 : 202004-086-C-RN, Received April 10, 2020; Revised May 15, 2020; Accepted June 9, 2020

Ⅰ. 서 론

미래 자동차들은 그룹 형태를 이루면서 주행에 필요한 정보를 상호 교환하거나 사용자의 컴퓨팅 환경을 위해서 내재 컴퓨팅 자원들을 공유하여 필요한 데이터들을 처리하는데 협력해 나간다[1].

차량 간 정보 교류에서 발생할 수 있는 문제점은 차량 내외에 존재하는 악의적 사용자의 잘못된 정보 유통을 통해 사고로 이어지거나 또는 비효율적인 운행을 유도할 수 있다. 따라서 차량 통신에 있어서 보안은 어떤 분야보다도 중요하다. 최근 블록체인은 블록에 데이터를 저장하고 해당 정보를 P2P 네트워크를 통해 상호 공유하고 합의 알고리즘에 의한 정보 동기화를 통해 데이터 무결성을 보장하는 시스템으로 주목받고 있다[5,6].

그림 1은 차량 포그/클라우드[1] 에서 블록체인을 이용한 차량 간 데이터 및 컴퓨팅 자원을 공유하는 예를 나타내었다. 기존 차량 블록체인기술[8]은 수집한 데이터를 저장하고 공유하며, 상호 검증을 통해 신뢰를 제공해 준다. 하지만 차량 블록체인은 합의 과정이 복잡하고 상당한 시간이 걸리므로 실시간 데이터를 교환해야하는 차량 통신에 어려움이 있다. 또한 퍼블릭 블록체인의 경우, 블록에 데이터를 쓰고 저장하는데 비용이 발생하므로 사용자들이 사용하기에 부담이 될 수 있다.

본 논문에서는 차량 클라우드를 위한 블록체인 구조를 제안하고, 차량 간 컨텐츠 쿼리 및 전송 방법과 결제 채널을 이용한 컨텐츠 결제 프로토콜을 제안 및 구현 하였다.

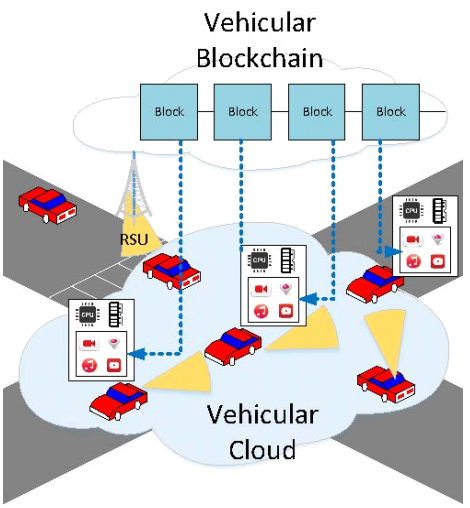


그림 1. 차량 블록체인 네트워크
Fig. 1. Vehicular blockchain network

Ⅱ. 결제 채널 네트워크

오프체인 기술은 2개 노드 사이에서의 트랜잭션 처리를 위해 생성한 상태 머신인 결제 채널을 이용한 결제 기술이다. 상기 결제 채널이 상호간 존재하지 않은 사용자 사이에도 다른 중간 사용자들의 결제 채널을 통해서 지불이 가능하다. 이를 멀티홉 네트워크를 결제 채널 네트워크라고 부르며 비트코인을 위한 라이트닝 네트워크나[4] 이더리움[2] 기반의 레이덴 네트워크[3] 가 있다.

결제 채널은 time lock이 가능하도록 설계된 애스크로우 계좌를 통해 생성된다. 블록체인에서 채널 사용자간 서명을 통해서 담보가 된 금액 만큼 상호 결제가 가능한 시스템이다. 따라서 상대방이 담보 금액 이상으로 결제를 시도할 경우에 받아 주지 않으므로 블록체인과는 달리 결제에 대한 인증 및 검증이 필요하지 않다. 다시 말해서 채널의 최종 상태에 대한 합의는 쌍방 간 이루어지므로 결제 처리 속도가 빠르고 블록체인에서의 블록 생성의 위한 합의 지연은 발생하지 않는다.

그림 2는 결제 네트워크에서 결제 절차를 나타내는 그림이다. 그림에서 노드 S는 노드 D에 $1에 해당하는 금액을 보내고자 할 때, time-lock이 된 조건부 지불 보증을 보낸다. 해당 지불은 포함된 secret 해쉬값을 포함하고 있어, 해당 pre-image를 나중에 노드 D로 하여금 전달 받게 되며 해당 secret 값을 통해 조건부 지불에 해당 하는 신규 지불 요청으로 정산을 할 수 있다. 만약 그림에서와 같이 해당 조건부 지급을 unlock 하고자 secret을 전달하였음에도 이전 노드가 조건부 지급에 대한 신규 지불을 수행하지 않는 경우에, secret 값과 가지고 있는 조건부 지급으로 블록체인에 분쟁해결 결차를 거쳐 정산할 수 있다. 하지만 블록체인을 통한 정산의 경우, 지불 채널 상태를 종료

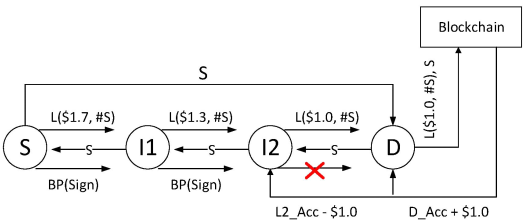


그림 2. 결제 채널 네트워크
Fig. 2. Payment channel network

하게 되어 추후 채널 개설에 대한 비용도 추가적으로 발생할 수 있어 가능한 모든 노드들이 정직하게 동작할 수 밖에 없다.

Ⅲ. 차량 클라우드 블록체인

본 장에서는 차량 포그에서 컨텐츠 교환을 위해 블록체인을 이용한 컨텐츠 관리, 쿼리, 전송 및 결제 채널을 이용한 결제 방안에 대해 제안한다.

3.1 블록체인 기반 컨텐츠 쿼리

그림 3는 차량 클라우드/포그 컴퓨팅에서 차량간 컨텐츠 교환을 위한 컨텐츠 쿼리 절차를 나타낸 그림이다. 컨텐츠 생성 차량과 소비 차량 사이에서 컨텐츠 정보에 대한 쿼리 과정에 따라 해당 컨텐츠의 위치를 파악하는 과정은 기존에 정보 중심 네트워킹 (Information centric networking)에서 주로 다루어 졌다[7]. 정보 중심 네트워크에서 크게 분산 컨텐츠 쿼리를 위해 제어 메시지들을 네트워크에 방송하는 형태의 프로토콜과 특정 노드들을 컨텐츠 정보 위치를 다루는 역할을 배정하는 방식이다. 본 차량 블록체인 네트워크에서는 컨텐츠 정보를 블록체인에 저장할 때, 해당 정보에 대한 호스트 정보, 가령 IP 주소, 또한 저장한다. 그림 3은 블록체인을 이용한 컨텐츠 쿼리 과정을 보여준다. 컨텐츠 제작 노드인 A가 컨텐츠의 메타 데이터 정보를 블록체인에 기록하고, 노드 A의 호스트 정보를 블록체인 계좌 정보로 저장한다. 이후에 차량 블록체인 노드들은 상기 정보를 저장 관리하고, light node 사용자 B가 컨텐츠 쿼리를 보내게 되면, 주위 full 노드들이 블록체인 내에 존재하는 컨텐츠 정보에 해당하는 호스트 정보를 전달해 준다. 이를 통해 사용자 B는 컨텐츠 위치를 확인할 수 있으며, 직접적으로 노드 A에 연결 요청을 하고, 데이터 전송을 받을 수 있게 된다.

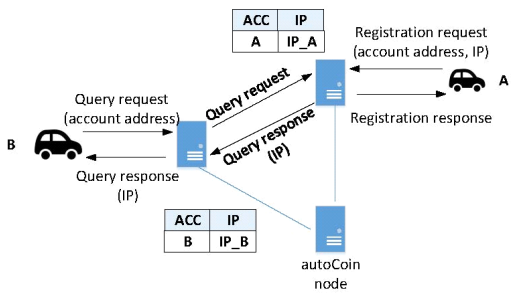


그림 3. 블록체인을 이용한 컨텐츠 쿼리 절차
Fig. 3. Procedure of content query using a blockchain

3.2 컨텐츠 정보 블록

차량 클라우드/포그 컴퓨팅에서 차량 안전 및 도로 상황 등에 관한 컨텐츠로 다양한 형태의 데이터가 존재할 수 있다. 대표적으로 차량에 장착된 비디오 캠에 의해 생성된 영상 컨텐츠를 고려해 볼 수 있다. 영상 데이터는 차량 운행 일지나 사고 기록으로도 사용될 수 있다. 그림 4는 블록체인 내에 차량 영상 컨텐츠의 메타 데이터 저장 방식을 나타낸다.

영상 데이터는 파일 크기가 매우 크므로 영상 데이터 자체를 블록체인에 저장하기 보다는 비디오 컨텐츠 해쉬 값을 블록에 저장하여 데이터 무결성을 보장한다. 또한 해당 트랜잭션의 내용을 보장하기 위해서 트랜잭션 해쉬 값도 블록에 기록된다. 해당 영상 정보로는 사용자가 정보를 쿼리하기 위해 필요한 메타 데이터들로 영상이 녹화된 시간, 장소, 크기, 가격 등이 될 수 있으며, 해당 컨텐츠 위치를 포함한다. 또한 co-sign 해쉬 값은 주변 차량으로부터 수신한 주소 값으로 촬영된 영상의 신뢰성을 높일 수 있다. 이후 컨텐츠 생성과 저장의 역할이 분리되면 컨텐츠는 분산 파일 시스템 (예로 IPFS (InterPlanetary File System))으로 참여 노드들에 분할되어 저장될 수 있다.

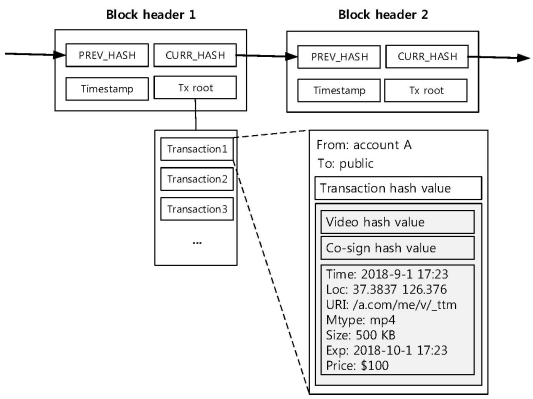


그림 4. 블록체인 내 컨텐츠 메타 데이터 정보
Fig. 4. Content meta-data in a blockchain block

3.3 컨텐츠 코인 패킷 프로토콜

그림 5는 차량 클라우드/포그 컴퓨팅에서 차량 간 컨텐츠 교환을 위한 코인 패킷 프로토콜 절차를 나타낸 그림이다. 컨텐츠 제작 및 보관 관리는 제한된 컴퓨팅 자원을 보유하는 차량에게 비용이 발생되는 동작이므로 이에 적절한 인센티브가 부여되지 않는다면 시스템 생태계를 유지하는데 어려움이 있다. 이에 기존 결제 채널 기술을 이용하여 코인 패킷을 구현하였다. 그림 5에서는 상기 오토코인 패킷을 이용한 컨텐

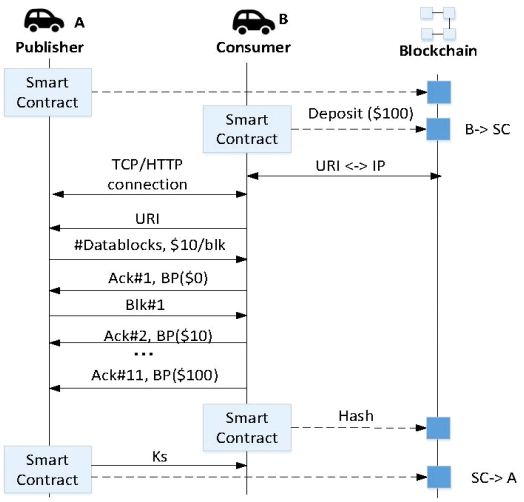


그림 5. 컨텐츠 코인 패킷 프로토콜
Fig. 5. Payment channel network

츠 전송 방법을 나타낸다. 기존 결제 채널 기술을 이용하여 스마트컨트랙트 (SC)를 이용하여, 차량 간 결제 채널을 생성한다. 그림 4에서 컨텐츠 생성자가 이미 생성한 컨텐츠에 대해 블록체인에 등록한 상태라면, 사용자 노드가 그림 4의 절차를 통해서 해당 컨텐츠의 호스트 정보인 노드 A 정보를 입수하게 된다. 이후 노드 B는 HTTP 통신을 이용하여 노드 A에게 해당 컨텐츠의 URI (Uniform Resource Identifier) 정보를 전송하여 컨텐츠 전달을 요청한다.

이 후 노드 A는 패킷 코인에 대한 사이즈 정보를 노드 B에게 알린다. 오토코인 패킷은 특정 패킷 코인에 대한 데이터가 encapsulation 된 형태로 토큰 정보와 컨텐츠 조각 (chunk) 이 하나의 패킷 형태이다. 해당 패킷을 수신 했을 경우에, acknowledgement 로 새로운 Balance Proof (BP) 에 대해 컨텐츠 제공자에게 보낸다. 따라서 각 데이터 패킷에 따른 과금이 가능하게 된다. 특정 컨텐츠의 경우, 데이터 일부를 통해 재생이나 사용이 가능할 경우에 정보 제공자는 해당 데이터를 암호화 할 수 있다. 해당 컨텐츠 암호화에 사용된 키는 정보 제공자에 의해 생성될 수 있으며, 해당 정보는 스마트 컨트랙트에 의해 정산 과정에서 사용자 노드에게 노출된다. 세부적인 절차로는 컨텐츠 사용자가 수신 받은 컨텐츠에 대해 해쉬 값을 생성하고 해당 해쉬값을 암호화에 사용된 대칭 공개키로 암호화하여 스마트 컨트랙트에 올리에 되면, 정보 제공자가 실제 사용한 컨텐츠 암호화 키, Ks를 스마트 컨트랙트에 컨텐츠 해쉬값과 같이 올린다. 스마트 컨트랙트는 해당 컨텐츠의 해쉬값과 암호를 비교하여 같을 경우, 키를 블록에 쓰고 정보제공자가 제공한 BP 금액을 해당 계좌로 이체시켜준다.

3.4 지역 사이드 체인

결제 채널 생성 및 컨텐츠 등록 관리를 위해서 차량 블록체인이 필요하다. 현재 블록체인 성능을 개선하기 위해서 다양한 멀티 체인 기술들이 적용되고 있다. 차량 블록체인은 차량 운행 및 안전 데이터 저장을 주목적으로 하고 있으므로 도로 및 지역에 기반한 계층적 블록체인이 적용 가능하다. 그림 6은 계층적 차량 블록체인 구조를 보여준다. 각 지역 도로를 기반으로 블록체인을 생성할 수 있으며, 해당 블록체인은 상위 매크로 지역의 블록체인과 연동하여 동작하게 되며, 최상위 root 체인의 경우, 기존의 공개 체인들과 연동될 수 있다.

하위 마이크로 체인에서는 해당 지역에서의 이벤트 트랜잭션들을 처리하게 되며, 상위 체인들은 하위 체인에서 발생한 블록들의 무결성을 보장하기 위해 해쉬값으로 구성된 블록들을 생성한다. 마이크로 체인에 참여하는 노드 수는 제한적이므로 블록을 생성하는 마이너는 상위 매크로 체인 중에서 임의로 선택된 마이크로 체인의 임의 노드가 담당한다. 이를 통해 마이크로 체인 내에서 노드 간 협력에 따른 데이터 조작을 방지한다. 마이크로 노드의 상위 체인으로 갈수록 체인에 참여하는 노드의 수는 증가하므로 블록 데이터의 신뢰도도 증가한다.

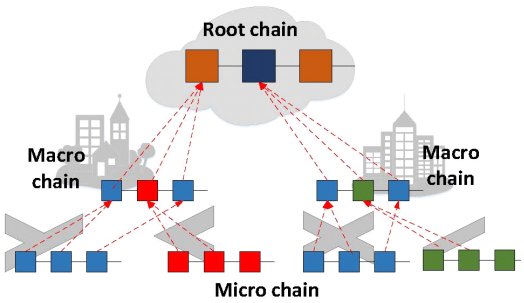


그림 6. 계층적 차량 블록체인 네트워크
Fig. 6. Hierarchical vehicular blockchain network

Ⅳ. 실 험

본 논문에서 제안하는 결제 채널과 코인패킷을 이용한 컨텐츠 결제 기능을 실검하고자 무선랜 AP 1개와 차량용 노트북 2개 (i5 2.3GHz, 8GB MEM), 블록체인 풀 노드로 아마존 클라우드 서버 3개 (Broadwell

E5-2686v4 and 8 GB memory) 를 이용하여 유사 차량 테스트 베드를 구성하였다. 이더리움[2]을 이용하여 사이드 체인 및 패킷 코인을 스마트 컨트랙트로 구현하였다. 그림 7과 같이 컨텐츠 및 코인패킷 전송을 위해 HTTP 프로토콜을 사용하였다. 차량 노드는 블록체인을 통해 컨텐츠 검색을 하고, 이를 기반으로 해당 노드에 HTTP를 이용하여 URI 요청을 보낸다. 차량 노드는 이를 위해 항시 HTTP 서버를 운용한다.

컨텐츠 전송에 있어 악의적 노드의 데이터 혹은 코인 패킷 스푸핑 및 재전송 공격은 암호화된 데이터나 해쉬 코인이 수신자의 전자서명이 필요하므로 안전하다. 패킷 수집을 이용한 무료 승차의 경우, 각 코인 패킷의 stage 혹은 round 값이 현재 채널과 다르고, 암호화 개인키가 랜덤 키로 재 생성되므로 새로 수신 받은 데이터를 사용이 불가하다. 하지만 재밍과 같은 DoS (denial of service) 공격은 결제 채널 분쟁 및 블록체인 접근으로 비용 발생을 유도시킬 수 있어 이에 대한 대책이 필요하다. 그림 8은 차량 블록체인 테스트베드에서 2개 노드 사이에서의 컨텐츠 전송/결제 시 발생하는 RTT (round trip time)를 측정한 값이다. 데이터 조각 당 발생하는 지연은 조각 크기에 비례하여 증가했다. 패킷 크기에 따라 처리 시간이 늘어나는 것을 확인했으나, 컨텐츠 전체 전송 시간 측면에서는 조각 크기가 큰 것이 유리하다. 하지만 데이터 조각 당 결제액이 커질 경우, 결제 채널 균형이 맞지 않을 수 있으며 결제 네트워크 성능이 저하될 수 있다. 처리 시간 측면에서는 정보 제공자 RTT가 크므로 정보 사용자에서 처리하는 시간이 길다. 주요 이유는 코인패킷이 HTTP로 구현되어 블록체인 모듈과 JSON RPC (remote procedure call) 을 통해 처리되는데 지연이

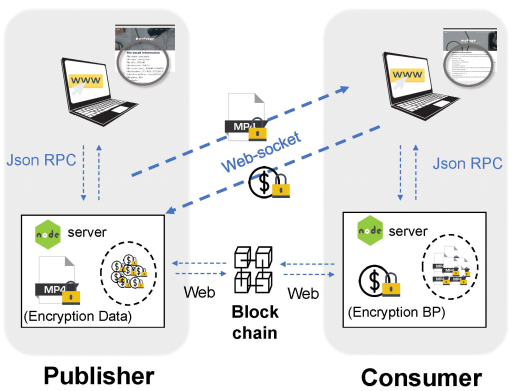


그림 7. 컨텐츠 결제를 위한 사이드 체인 및 코인 패킷 구현
Fig. 7. Side-chain based coin packet implementation for content payment

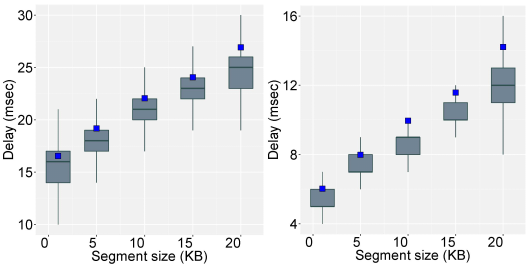


그림 8. 컨텐츠 결제 지연 측정 (좌측: 정보제공자, 우측: 정보사용자)
Fig. 8. Delay measurement for content payment

발생했다. 이는 light node의 경우 추가적으로 발생할 수 있는 지연이며 full node의 경우 해당 지연을 줄일 수 있다. 100 MB 데이터를 전송하는데 2분 정도의 시간이 소요되었으며 5G 차량통신 적용에 따라 전송 시간이 줄어들 수 있다.

V. 결 론

본 논문에서는 차량 클라우드에서 데이터 보안 및 교환을 위한 블록체인 기반 프레임워크를 제안하고, 컨텐츠 거래에 필요한 결제 채널 프로토콜을 설계하였다. 테스트베드 구현을 통해 제안 프로토콜이 컨텐츠 거래에 사용될 수 있음을 확인하였다.

References

[1] M. Gerla, “Vehicular cloud computing,” *2012 The 11th Med-Hoc-Net*, 2012.

[2] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, no. 1, 2014.

[3] Raiden network, “https://raiden.network,” 2018.

[4] J. Poon and T. Dryja, “*The bitcoin lightning network: Scalable off-chain instant payments*,” lightning-network-paper-DRAFT-0.5, 2015.

[5] S. Lee and J.-H. Lee, “TEE based infotainment session key establishment protocol using blockchain,” *J. KICS*, vol. 43, no. 12, pp. 2114-2121, 2018.

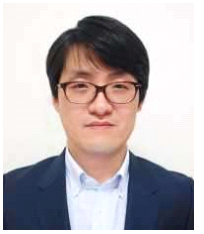
[6] C. Jang and O. Yi, “Blockchain network configuration for smart contract in ev charging infrastructure,” *J. KICS*, vol. 44, no. 8, pp. 1597-1604, 2019.

[7] W. Kim, “Beyond LTE-advance for

information centric networking," *Computer Standards & Interfaces*, vol. 49, 2017.

[8] Z. Yang, et al., "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things J.*, vol. 6, no. 2, pp. 1495-1505, 2018.

김 우 성 (Wooseong Kim)



2000년 2월 : 서울시립대학교 전기전자공학과 학사

2004년 2월 : 한국과학기술대학교 정보공학과 석사

2012년 3월 : UCLA 컴퓨터 과학 박사

2015년 3월 : 현재 가천대학교 부교수

<관심분야> 블록체인, P2P 네트워크, 5G 이동통신

[ORCID:0000-0003-0955-3421]