디지털산업정보학회 논문지 제14권 제3호-2018년 9월
http://dx.doi.org/10.17662/ksdim.2018.14.3.069

# M2M 환경의 혼잡 네트워크 개선을 위한 블록체인 경량화에 대한 연구

김 상 근*

# *A Study on the Lightening of the Block Chain for Improving Congestion Network in M2M Environment*

Kim Sanggeun

〈Abstract〉

Recently, various convergence technologies are attracting attention due to the block chain innovation technology in the M2M environment. Although the block-chain-based technology is known to be secure in its own right, there are various problems such as security and weight reduction in various M2M environments connected with this. In this paper, we propose a new lightweight method for the hash tree generation of block chains to solve the lightweight problem. It is designed considering extensibility without affecting the existing block chain. Performance analysis shows that the computation performance increases with decreasing the existing hash length.

Key Words : M2M, IoT, Blockchain, Hash Chain, Device Authentication

## Ⅰ. 서론

블록체인(Block Chain) 기술은 2008년 사토시 나카모토(Satoshi Nakamoto)에 의해 개발된 비트코인(Bitcoin)이라는 가상화폐의 거래 장부 기술로 개발되었다[1]. 기존 PKI(Public Key Infrastructure)와 같이 신뢰 된 제3기관을 통한 상호인증 기술과는 차이점이 있다. 완전한 P2P(Peer to Peer) 네트워크상에서 분산된 사용자 간의 상호인증을 통해 거래 신뢰성을 확보할 수 있으며, 또한 이중 지불 방지와 사용자의 익명성을 보장한다. 최근 M2M(Machine-to-Machine) 또는 IoT(Internet of Things) 등 기존 블록체인 기반기술이 시장에서 확장되면서 다양한 방법으로 응용되고 있다. 기존 PC, 모바일 결제시장에서 자동차, 항공, 선박 등 실생활로 확대되면서 사물인터넷을 구성하는 수십 억대 장치가 네트워크를 구성할 것으로 예상한다[2]. 분산원장이라는 특징을 가진 블록체인 기반 네트워크는 많은 문제점이 존재한다. 가장 큰 문제는 데이터의 수집 및 전송 가용성과 효율성이 기존 네트워크 환경보다 성능이 떨어진다는 사실이다[3,4].

본 논문에서는 M2M과 같은 새로운 환경에서 기존 블록체인이 적절하게 활용되기 위한 경량화된 해시 체인 트리생성에 대한 방법을 제안한다. 본 논문은 모두 5장으로 구성된다. 2장은 기존 블록체인 기

* 성결대학교 컴퓨터공학부 교수

술과 M2M 환경에서 해시 트리 적용 문제점을 분석한다. 3장은 경량화된 블록체인 해시 트리생성 방법을 제안한다. 4장은 기존 환경과 제안하는 기법을 비교분석 5장은 결론을 맺는다.

## Ⅱ. 관련연구

### 2.1 국·내외 블록체인 시장 현황 분석

전 세계적으로 R3CEV(Crypto, Exchanges and Venture Practice)와 Hyperledger 프로젝트를 중심으로 세계 주요 금융사가 참여 중이며, 유럽에서는 HSBC 등 대형 은행을 중심으로 DTC(Digital Trade Chain), 국내에서는 금융위원회 주관 하에 금융권 공동 블록체인 컨소시엄이 운영 중이다[5]. 표 1은 주요 산업별 블록체인 활용 사례를 나타낸다[6].

<표 1> 산업별 블록체인 활용 사례[6]

| 분야 | 사례 |
|---|---|
| 증권 거래 | 블록체인 기반의 거래 플랫폼을 제공, 효율성을 위한 시스템을 개발 중 |
| 청산결제, 송금 | 정부에서 거래 관리, 다양한 통화와 가상화폐(비트코인, Ether 등) 플랫폼 개발중 |
| 투자/대출 | 투자자와 스타트업 기업을 연결해 투자금을 확보하기 위한 플랫폼 제공 |
| 상품 거래소 | 블록체인 기반 거래 플랫폼의 자산과 금융상품 거래 기능 제공 |
| 무역금융 | 무역거래 시 이용되는 문서의 위변조 방지, 처리절차 간소화 등에 적용 |
| 관리(규정 등) | 블록체인 거래에 관한 규정의 준수 여부를 모니터링 하는 기능 제공 |

주요 스타트업은 대부분 블록체인을 활용한 금융 분야이며, 기타 비금융 분야로는 신원관리, 공증, 소유권 증명, 투표 등의 기술로 확대되고 있다[6]. 핵심 개발 플랫폼이 대부분 금융 분야를 중심으로 진행되고 있다. 기존 거래 기능보다 M2M 환경에서 확장된 기능으로 적합한 유통 또는 수송 항목은 기타 산업으로 분류하고 있다. 이는 현재 블록체인 기반 M2M 시장이 아직 초기임을 나타낸다. 표 2는 기타 산업별 블록체인 활용 사례를 나타낸다[6].

<표 2> 기타 산업별 블록체인 활용 사례[6]

| 분야 | 사례 |
|---|---|
| 신원관리 | 신원 정보를 블록체인에 저장 및 신원확인 데이터 유효성, 활동 분석 등 신원 정보 관리 기능 제공 |
| 공증/소유권 | 공증, 소유권 등과 관련된 분쟁 소지 (문서 위·변조 등) 방지를 위한 검증, 인증, 사기탐지 등의 기술 개발 |
| 전자투표 | 전자투표의 신뢰성 및 투표과정을 제공하여 선거 시스템에 대한 투명성 제공 |
| 수송 | GPS를 이용하여 차량의 움직임으로 토큰 생성 |
| 유통 | 상품, 재고 관리 등의 전산화, 중개기관을 대체하는 거래 플랫폼 개발 |
| 보안 | 상품 위변조, 접근 권한, 기기 관리 등 정보 관리 기능 개발 |
| 스토리지 | 데이터를 분산하여 저장하는 기술 개발 |

실생활에 가까운 M2M 장치로는 차량 관련 산업에 기대가 가장 관련이 높았고, 세부분야에 친환경 전력거래를 위한 스마트계약 개발과 사물인터넷을 위한 블록체인 연결이 핵심 사례이다. 국내 블록체인 스타트업 사례를 살펴보면 삼성전자 SDS의 해운물류 블록체인 컨소시엄이 대표적이며 공공 이외에 중소·민간 분야까지 산업이 활성화하는데 시간이 필요할 것으로 분석된다. 향후 수억대 이상의 진정한 M2M 네트워크를 실현하기에는 현재 아직 시장이 초기이고, 기술 단계가 미성숙한 단계로써 국내

외 많은 연구와 투자가 요구됨을 알 수 있다.

## 2.2 M2M 환경에서의 문제점 분석

M2M 환경의 블록체인 기술 개발에 앞서 블록체인에 대한 규제와 각 국제기구, 주요국 정부와 중앙은행들의 법·제도적인 부분이 표준화가 선행되어야 한다. 주요국마다 각각 다른 디지털 통화와 규정을 준수하기 때문에 문제점 분석은 국내 시장의 흐름에 따른 기술 문제점을 가정한다. 국내의 경우 주요 은행들을 중심으로 블록체인 기술을 활용하기 위한 제휴 및 기술 개발에 본격적으로 나서고 있다.

일반적으로 알려진 주요 이슈는 분산원장 기술의 특징으로 거래에 대한 보안성과 성능이다. P2P 블록체인 네트워크 구성으로 인한 연산속도 저하 문제는 지속해서 이슈가 되어왔다. 최근 국내에서는 은행권을 중심으로 블록체인 인증 서비스를 시범적으로 운영 중이다[7].

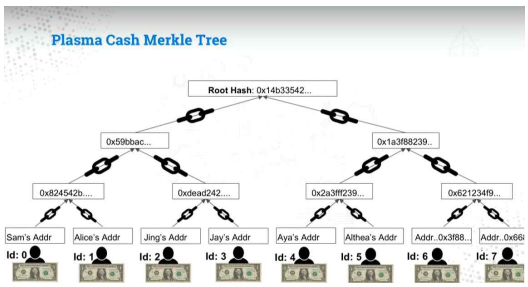
<표 3> 퍼블릭 블록체인과 프라이빗 블록체인

| | 퍼블릭 블록체인 | 프라이빗(컨소시움) 블록체인 |
|---|---|---|
| 읽기 권한 | 누구나 열람 가능 | 허가된 기관만 열람 가능 |
| 거래 검증 및 승인 | 누구나 네트워크에 참여하면 거래 검증 및 승인을 수행 | 승인된 기관과 감독 기관 |
| 트랜잭션 생성자 | 누구나 트랜잭션을 생성 | 법적 책임을 지는 기관만 참여 |
| 합의 알고리즘 | 부분 분기를 허용하는 작업증명이나 지분증명 알고리즘 | 부분 분기를 허용하지 않는 BFT계열의 합의 알고리즘 |
| 속도 | 7~20TPS | 1000 TPS 이상의 고성능 |
| 권한 관리 | 누구나 모두가 모든 일을 할 수 있음 | Private Channel, Tierd system 등을 통해 읽기 쓰기 권한 관리가 가능 |
| 예시 | 비트코인, 이더리움 | IBM Fabric, LoopChain, R3 Corda |

이는 대표적인 사례로 공개 입찰을 통해 삼성 SDS 넥스레저(Nexledger)를 도입 결정했다[8]. 넥스레저는 오픈소스 기반으로 자체 개발된 블록체인 플랫폼으로써 퍼블릭 블록체인이 아닌 프라이빗 블록체인 영역으로 분류된다. 표 3은 퍼블릭 블록체인과 프라이빗 블록체인의 차이점을 나타낸다[9].

성능 부분을 개선하기 위해 직접 트랜잭션을 최적화한 것으로 알려져 있다. 프라이빗 블록체인을 선택했다는 것은 기존 느린 성능의 문제점이 시범서비스에는 역시 부담될 수밖에 없으므로 적합한 선택이라고 볼 수 있다. 그러나 프라이빗 구조로도 실제 대규모 시스템 구축이나 은행권에 대한 보안성, 안전성이 아직 검증된 것은 아니다[10,11]. 이는 은행권을 대상으로 예상되는 한계 거래량을 고려하여 플랫폼을 개발한 것이기 때문에 그 규모가 차원이 다르게 확장되고, 복잡도가 높아지는 M2M 환경에는 역시 적합하지 않다고 할 수 있다. 현재 기술 수준으로는 결국 M2M 환경에 퍼블릭 블록체인 속도저하를 고려하여 플랫폼이 개발되어야 할 것이다. 이는 블록체인 자체에 대한 성능 개선보다 원초적으로 구조 자체를 개선해야 할 필요가 있다는 것이다. 또는 블록체인을 처리하는 IoT 장비들의 하드웨어 수준이 개선되는 방법이 필요한데, 이는 장비의 성능 요구사항이 정의되는 표준화 심화 단계까지 진입하는 데는 수년 이상이 걸릴 것으로 예상한다[12].

일반적으로 블록체인의 성능 문제점에 대한 해결책은 3가지 정도로 고려해 볼 수 있다. 첫째 초기 블록체인의 생성 길이 자체를 최소화하여 트랜잭션에 드는 비용 자체를 감소시킨다. 둘째 이미 생성된 블록체인의 트랜잭션 생성과 검증의 비용을 최적화한다. 셋째 트랜잭션의 암호학적 알고리즘 연산을 경량화 한다. 그림 1은 최근 대표적인 블록체인 기술로 알려진 이더리움의 발전된 형태인 플라즈마 캐시의 구조를 나타낸다[13].




<그림 1> 개선된 블록체인 플라즈마 캐시[13]

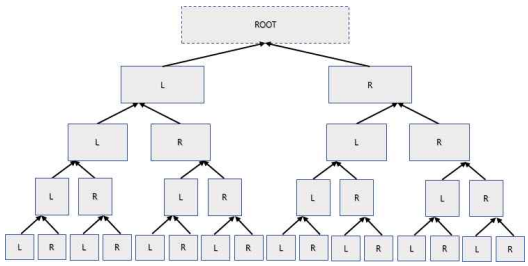
최근 이더리움의 창시자 비탈릭 부테린(Vitalik Buterin)은 기존 성능의 한계를 극복하기 위해 트랜잭션 비용을 줄이는 플라즈마 캐시를 이더리움 커뮤니티 콘퍼런스(EhtCC)에서 발표했다[13]. 기존 프로토타입의 플라즈마 블록체인의 무거운 검증, 불편한 거래방법, 대응책의 부재 등 문제점을 일부 개선하였다. 이는 기존 분산원장 기술의 최적화가 M2M과 같은 환경에 적절한 형태로 새롭게 구조적인 변화를 시도해야 한다는 시점에 왔다는 것을 의미한다.

## Ⅲ. 개선된 블록체인 구조

### 3.1 이중 머글트리 생성

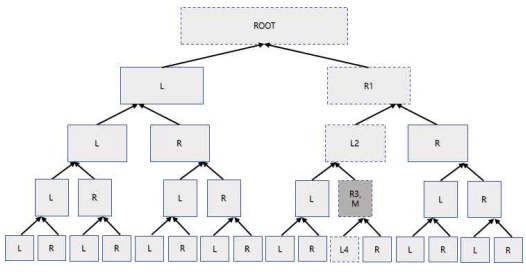
본 논문에서는 현재 블록체인 또는 이더리움에서 사용하는 머글트리를 사용한다. 현재 블록체인 거래의 수 기가에 달하는 거래내용 위변조를 확인하는 트랜잭션을 최적화하기 위해 이중 머글트리를 생성한다. 내부 해시 알고리즘으로는 기존 블록체인 호환성을 위해 SHA256와 이진트리를 그대로 적용한다. 그림 2는 기본 머글트리 전체구조를 나타낸다. 기존 머글루트(ROOT)를 포함하고 블록의 깊이에 따라 왼쪽(L), 오른쪽(R)로 표현하였다.

블록체인 전체를 포함하는 풀 노드(FullNode)의 연산비용을 감소시키기 위해서 라이트 노드(Lightweight)에 요약된 마스터 노드 개념을 추가 적용한다. 라이트 노드는 일반적으로 PC, 웹 제공자, 모바일 등에서 사용하는 지갑(Wallet) 기능을 수행하는 노드이다. 대부분 사용자가 풀 노드 기반 지갑을 직접 사용하지 않기 때문에 지갑의 라이트 노드를 활용하여 검색, 검증 등 기능을 빠르게 수행하도록 설계되었다.




<그림 2> 기본 머글루트 구조

본 논문에서는 지갑 역할을 다른 곳에서 수행하는 Web Node의 경우는 제외한다. 트랜잭션의 최적화로 인한 연산비용 감소는 블록체인 보안에 큰 문제가 될 수 있기 때문이다. 이외 사용자가 패스워드(개인키)를 안전하게 보관·유지한다고 가정한다. 그림 3은 머글트리에 요약된 라이트 노드 부분(깊이를 숫자로 표현)과 마스터 노드(M) 위치를 추가하였다.




<그림 3> 마스터 노드가 추가된 머글루트 구조

점선으로 추가 표현된 부분은 정상적인 머글루트(R1, L2, R3_M, L4)인 경우를 나타낸다. 마스터 노드(M)로부터 블록체인 마지막까지 깊이와 경로(방향)를 요약한 헤더 정보를 추가 저장한다. 이는 법적 책임을 지는 기관만 트랜잭션을 생성할 수 있는 권한을 부여한다. 즉, 퍼블릭 블록체인을 유지하면서 관리 주체가 블록체인의 생성과 트랜잭션 처리를 관리하는 형태이다. 표 4는 각 주체와 노드의 역할을 나타낸다.

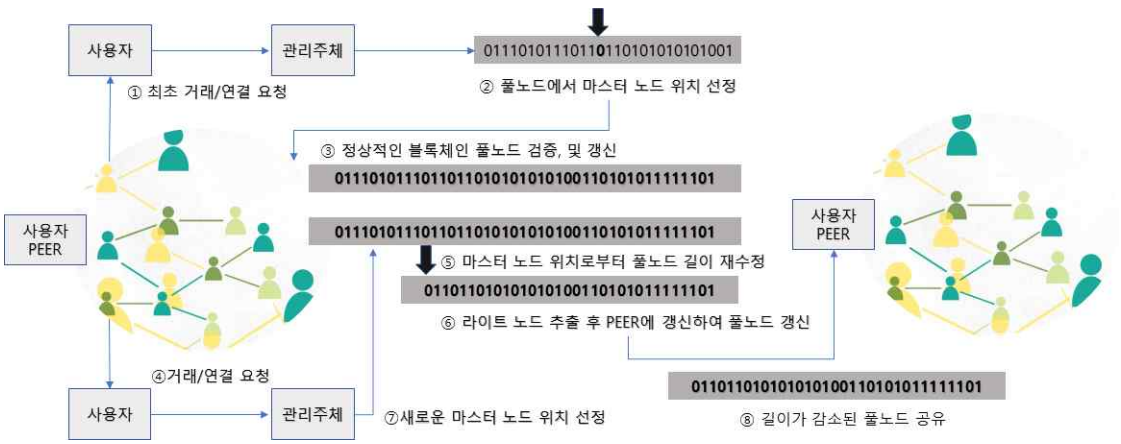
<표 4> 각 주체와 노드의 역할

| 항목 | 설명 |
|---|---|
| 사용자 PEER | 거래/연결 검증 및 갱신 |
| 관리주체 | 마스터 노드(M) 위치 요약헤더 |
| 풀 노드 | 전체 블록체인 |
| 라이트노드 | 머글트리 요약헤더 |

## 3.2 분리된 거래검증(합의)

기존 P2P 네트워크는 모든 거래에 대해 블록체인 해시 값을 변경해야 하는 구조이다. 이는 블록체인 길이가 증가할 수밖에 없고, 갱신과 검증에 큰 비용이 요구된다. 분리된 거래검증은 거래 초기에 최소한 한 번 이상 블록체인을 생성해야 한다. 차이점은 선택된 마스터 노드를 기준으로 블록체인의 검증을 수행하여 머글트리를 검색하는 연산비용을 최적화하는 것이다. 그림 4는 기존 풀 노드 블록체인이 존재한다는 가정하에 전체 거래검증 과정을 나타낸다.

관리 주체는 마스터 노드가 요약된 헤더를 보유한다. 사용자 PEER 상에서는 마스터 노드의 위치를 알 필요가 없다. 최초 거래/연결 요청에서 관리 주체는 마스터 노드부터 블록체인의 시작으로 설정하고 P2P 네트워크에 전체 블록체인 정보를 갱신하게 된다. 이후 사용자 요청에서 관리 주체는 라이트 노드의 요약 헤더로부터 마스터 노드 위치를 참조한다. 이는 풀 노드 시작이 아닌 마스터 노드 시작 위치로부터 블록체인을 검증하여 트랜잭션의 비용을 최적화할 수 있다. 또한, 거래금액의 양이나 네트워크의 중요도 또는 사용자 선택에 따라 마스터 노드의 위치로부터 새로운 풀 노드를 구성하여 공유하면 기존의 수십 기가가 되는 블록체인 길이를 획기적으로 줄 일 수 있다.




<그림 4> 전체 거래검증 과정

### 3.3 이중 머글트리 성능분석

성능분석에서 기존 생성된 블록체인의 머글트리(이진트리를 예) 풀노드 생성 비용은 제외한다. 표 5는 M2M 환경에서 새로운 장치 또는 네트워크 구성으로 인해 블록체인 연결이 약 1000개 추가 생성되었을 경우 비용의 예를 나타낸다.

<표 5> 마스터 노드 깊이에 따른 최종 블록체인 길이 예)

| 머글트리 헤더 | 마스터 노드(M) 깊이 | 추가 블록체인 길이 | 재구성된 후 블록체인 길이 | 최종 블록체인 길이 |
|---|---|---|---|---|
| - | 1000 | 5KB × 1000개 = 5MB | 변화 없음 | 505MB |
| 제안 기법 적용 후 | 850 | | 425MB | 430MB |
| | 800 | | 400MB | 405MB |
| | 750 | | 375MB | 380MB |
| | 700 | | 350MB | 355MB |
| | 650 | | 325MB | 330MB |

기존 500MB 블록체인 풀노드가 존재하는 경우, 추가되는 블록체인 길이(헤더 및 데이터 포함)를 최소 5KB(1000회 = 5MB)로 가정하였다. 마스터 노드(M)의 위치는 전체 블록체인 기준의 상대 위치 의미한다. 본 논문의 제안 머글루트 헤더는 요약정보를 이중으로 생성한다. 예를 들어 750 위치의 마스터 노드 헤더는 훨씬 가까운 상대 위치로부터 해쉬 트리 구조를 탐색하여 네트워크 연결의 무결성과 유효성을 빠르게 검증한다. 또한, 최종 블록체인을 마스터 노드 기준으로 재구성하여 길이를 감소시킨다. 즉, 초기 블록체인 길이는 지속해서 증가하겠지만, 전체 오버헤드가 커져 적합하지 않은 시점이 올 것이다. M2M 네트워크 환경에 적합한 수준으로 최종 블록체인 길이를 감소시키는 방법은 전체 네트워크를 효율적으로 관리하기 위해 필수 요소라고 할 수 있다.

## Ⅳ. 결론

M2M 환경에서 지속해서 증가하는 블록체인의 길이와 연산비용은 큰 문제점으로 인식되고 있다. 본 논문에서는 M2M 환경에서 트랜잭션을 최소화하고 블록체인 길이를 감소시키기 위해서 이중 머글트리를 생성하고 마스터 노드를 따로 적용하는 분리된 거래검증을 제안하였다. P2P 네트워크로 구성된 전체 노드에 정보를 공유하는 것은 기존 블록체인 네트워크 구조와 큰 차이가 없지만, 블록체인 자체를 재구성하여 감소한 길이의 블록체인을 네트워크에 다시 재공유하는 방법은 기존 구조와는 크게 차이점이 있다. 이는 관리주체가 특정 노드에 대한 정보를 마스터 노드로써 보유하고 재구성된 풀노드를 관리할 수 있으므로 가능한 것이다. 이중 머글트리는 금융권에서 주요 기능인 거래보다는 실시간으로 빠른 처리가 요구되는 물류/수송 등에 대규모 네트워크를 관리하는 데 적합하다고 할 수 있다.

향후 연구로는 최적화된 블록체인 구조에 대한 보안 문제를 분석하는 것이다. 본 논문에서 제안한 마스터 노드 위치는 전체 해시 연산 성능에 영향을 끼치기 때문에 보안에 큰 영향을 끼칠 수 있다. 이는 거래/연결 요청뿐만 아니라 블록체인의 최소/최대길이와 갱신지연 설정 또는 거래종료로 인한 세션 종료 후 블록체인에 대한 관리적 정책이 추가로 요구될 것이다.

## 참고문헌


[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] 신용우, “블록체인 기술 현황 및 산업 발전을 위한 향후 과제,” 국회입법조사처, 이슈와 논점, 1476호, 2018, pp.1-2.

[3] 강승준, “블록체인 기술의 이해와 개발 현황 및 시사점,” 소프트웨어산업진흥본부, 이슈리포트 제13호, 2018, pp.13-14.

[4] 유순덕, 신성영, “블록체인 기반의 의사결정 사례 및 시사점,” 한국정보화진흥원, ICT 신기술, 2018, pp.16-17.

[5] 강준영, “블록체인 2.0의 출현과 금융시장의 변화,” 미래전략개발부, 제742호, 2017, p.13.

[6] 박정호, “블록체인 산업 현황 및 동향,” 소프트웨어산업진흥본부, 이슈리포트, 제17호, 2018, pp.7-9.

[7] 방태웅, “4차산업혁명의 기반기술, 블록체인,” 융합연구정책센터, 융합 Weekly TIP, vol.108, 2018, p.4.

[8] 조주현, “블록체인(Block Chain)이 기업의 경쟁력을 바꾼다!,” 포스코경영연구센터, POSRI 이슈리포트, 2017, p.1.

[9] 유진호, “loopchain – 블록체인으로 진짜 서비스 만들어보기,” the loop, 2017, p.9.

[10] 최희식, 조양현, “비트코인에 대한 안전성 확보를 위한 문제점 분석,” 디지털산업정보학회 논문지, 제13권, 제3호, 2017, pp.1-2.

[11] 이세열, “블록체인을 적용한 사설 클라우드 기반 침입시도탐지,” 디지털산업정보학회 논문지, 제14권, 제2호, 2018, pp.11-12.

[12] 차홍기, 이원석, 최영환, 이주철, 이강찬, “블록체인 국제표준화 동향,” 정보통신기술진흥센터, 주간기술동향, 2018, pp.11-13.

[13] Karl Floersch, “Ethereum scaling : Plasma & shading,” Ethereum Community Conference, 2018.


■ 저자소개 ■


김상근
(Kim Sanggeun)

1996년 3월~현재
성결대학교 컴퓨터공학부 교수
2003년 - 2004년
Sydney University 방문교수
1996년 2월
중앙대학교 컴퓨터공학과 (공학박사)
관심분야 : 정보보안, 핀테크, 빅데이터
E-mail : sgkim@sungkyul.edu



논문접수일 : 2018년 08월 23일
수 정 일 : 2018년 09월 03일
게재확정일 : 2018년 09월 04일