Journal of KIIT. Vol. 18, No. 4, pp. 9-19, Apr. 30, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.4.9

공개마켓 플레이스를 위한 블록체인의 RDB 구현 방법 연구

강희복*, 장창수**

A Study on RDB Implementation Method of Blockchain for Openmarket Place

Hee-Bog Kang*, Chang-Soo Jang**

요 약

본 논문은 쿼리 기능을 갖고 있는 RDB(Relation Database) 형태의 블록체인을 구성하여 공개마켓에 적용하기 방법을 제안한다. 비트코인은 네트워크 유지를 위한 방법으로 채굴에 의한 보상 방식을 사용하고 있기 때문에 처리시간은 7TPS(Transaction Per Secound) 속도로 제한한다. 그러나 본 논문에서 제시한 오픈마켓을 위한 블록체인은 한 블록에 한 거래만 기록하는 OTPB(One Transaction Per Block) 알고리즘과 처리시간에 제한을 두지 않고 경쟁 없이 블록을 생성하는 ACAB(Automatic Consensus Automatic generated Block hash value) 알고리즘을 적용하였다. 동일한 조건에서 파일 유형과 RDB 유형의 블록체인을 실험한 결과 파일 유형 블록 체인은 블록수가 증가함에 따라 속도가 느려지고 메모리 사용량이 증가했다. 그러나 RDB 유형의 블록체인은 일정한 속도와 메모리 사용량을 유지하였다. 따라서 RDB 유형 블록체인은 복잡한 비즈니스 모델에 적합하다는 결론을 얻었다.

Abstract

In this paper proposes a method of constructing an RDB(Relation Database) type blockchain that has a query function and applying it to the public market. Bitcoin uses a compensation method by mining as a method for network maintenance, so the processing time is limited to 7TPS (Transaction Per Secound) rate. However, the block chain for the open market proposed in this paper is an OTPB (One Transaction Per Block) algorithm that records only one transaction per block. And without limitation on processing time the ACAB (Automatic Consensus Automatic generated Block hash value) algorithm that generates blocks without competing was applied. As a result of experimenting the file type and RDB type blockchain under the same conditions, the file type blockchain slowed down and the memory usage increased as the number of blocks increased. However, the RDB type blockchain was maintained with a constant speed and memory usage. Therefore, it was concluded that an RDB type blockchain is suitable for a complex business model.

Keywords

blockchain, blockchain RDB, openmarket place, automatic consensus, automatic mining, AI chatbot

* 전남대학교 컴퓨터공학과 박사과정
- ORCID: https://orcid.org/0000-0001-8098-6006
** 전남대학교 컴퓨터공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-3517-3019

· Received: Nov. 21, 2019, Revised: Apr. 20, 2020, Accepted: Apr. 23, 2020

· Corresponding Author: Chang-Soo Jang
Chonnam University 2th gong-hakgwan 4 flor, 50 Daehak-ro, Yeosu-si, Jeollanam-do, 59626, Korea.
Tel.: +82-61-659-7251, Email: csjang@jnu.ac.kr

Ⅰ. 서 론

블록체인은 데이터를 거래할 때 중앙집중형 서버에 기록을 보관하는 기존 방식과 달리 거래 참가자 모두에게 내용을 공개하는 분산디지털 장부를 말한다[1]. 블록체인에 참여한 모든 구성원이 P2P네트워크(Peer-to-Peer Network)를 통해 서로 데이터를 전송, 검증, 저장하고 공유함으로써 공격자가 특정 데이터를 조작하더라도 대다수의 다른 참여자의 데이터까지 동시에 조작할 가능성이 낮아지기 때문에 이러한 분산 장부를 통해 높은 보안성. 확장성. 투명성 등이 보장 된다[1].

블록체인의 장점인 저비용 P2P 네트워크[2]와 분산 장부를 활용하면 중앙집중형으로 운영되는 공개마켓을 대체하는 완전한 형태의 공개마켓 플레이스를 구축할 수 있다. 완전한 형태의 공개마켓 형태는 각 노드마다 독립 마켓을 운영하며 상품을 등록하면 P2P 네트워크를 통해 다른 노드의 블록체인에 상품을 추가해 나가는 것이다. 각 노드마다 마켓을 통해 모집된 회원정보도 다른 노드와 공유하게 되면 소형의 독립 마켓은 블록체인을 통해 그림 1과 같은 거대한 가상 마켓을 구성하게 된다.

오픈마켓은 상품 검색에서 랜덤 검색과 연관검색을 할 수 있는 쿼리(Query) 기능이 필요하므로 블록에 상품정보를 쿼리 하기 위해서는 기존의 Key-Value 방식의 File DB로 구성된 블록체인을 RDB (Relation Database) 방식의 블록체인으로 구현하는 방법을 연구할 필요성이 있다.

본 논문에서는 블록체인을 비즈니스 모델에 적용하기 편리한 방법을 구현하기 위해 RDB로 블록체인을 구현하는 이외에 거래발생과 동시에 블록을 생성하여 처리시간을 단축하는 방안으로 하나의 블록에 하나의 거래를 기록하는 그림 2의 구조를 갖는 OTPB(One Transaction Per Block) 알고리즘과 블록 해쉬 값 자동생성용 ACAB(Automatic Consensus Automatic Block) 알고리즘을 사용하여 채굴 기능을 대체시키는 방법을 제안하였다.

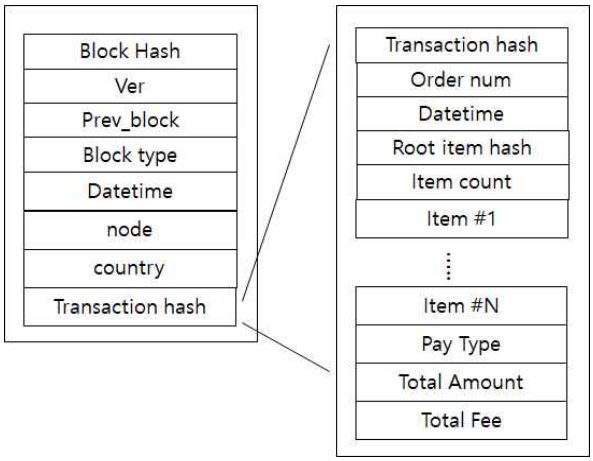

그림 2. OTPB 모델
Fig. 2. One transaction per block model

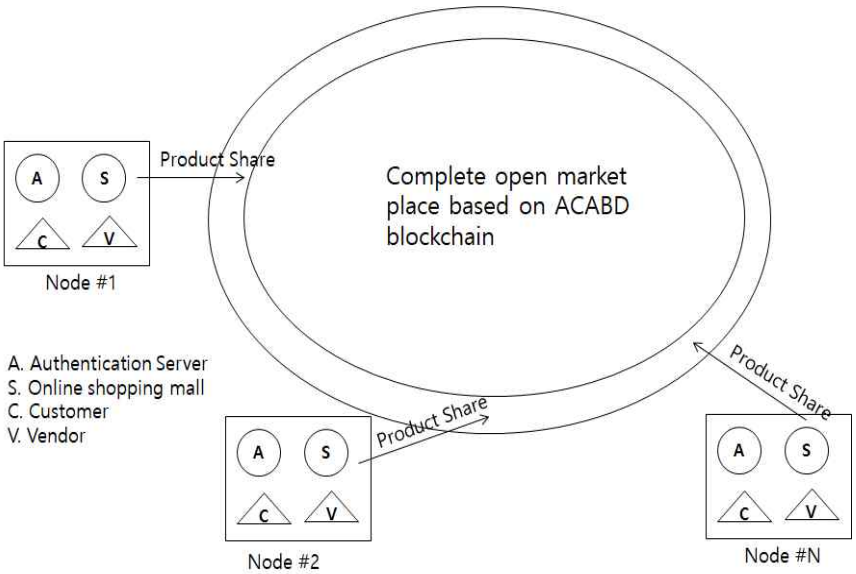

그림 1. 블록체인 기반의 완전한 공개마켓 플레이스 개념
Fig. 1. Block-chain based complete open-market place concept

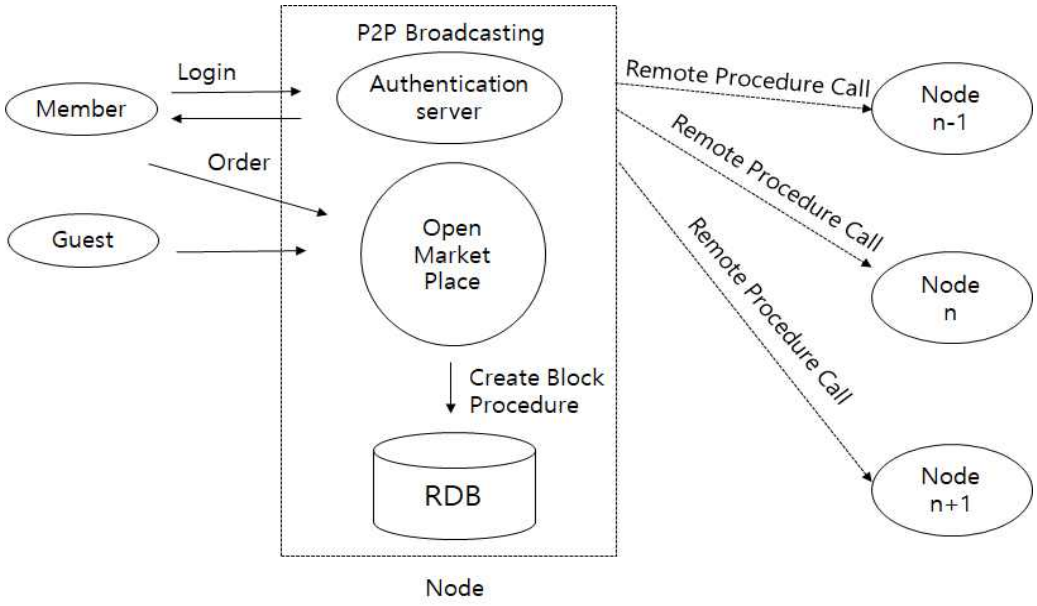

그림 3. ACAB 프로세스
Fig. 3. ACAB process

그림 3은 노드 역할을 하는 마켓에서 주문거래가 발생하면 노드의 인증서버에 등록된 참가노드의 IP와 순차 연결하고 ACAB 알고리즘에 의해 자동 합의를 수행하는 프로세스를 보여주고 있다.

로그인 한 구매자는 인증 서버에서 IUWT 토큰을 발급하고 IP주소 또는 단말기의 UUID 변경이 없는 경우 자동 로그인 처리 된다[3].

논문의 제 2장에서는 블록체인을 공개마켓 플레이스에 적용하기 위한 문제점과 필요성을 고찰하였고 제 3장은 ACABD 블록체인에서 거래와 블록을 구성하는 방법인 OTPB 및 노드에 의한 채굴 기능 대신 인증 서버가 원격의 노드와 P2P 네트워크로 연결하여 합의에 해당하는 최종 블록 검사와 새로운 블록 값 자동 생성 및 블록에 거래를 포함시키는 ACAB 방법에 대하여 기술하였으며 제 4장은 ACABD 블록체인이 공개마켓 플레이스에서 노드와 인증 서버 및 마켓을 구성하는 방법에 관해 기술하였고 본 논문에 적용한 RDB에 블록을 생성하는 것이 기존의 File DB(DB4)에 비해 빠르며 파일 크기도 작다는 것과 랜덤 검색에서 메모리 사용량이 안정적인 것을 확인하였다. 기존의 블록체인이 7 TPS 속도를 갖는 것[4]에 반해, 하나의 블록은 하나의 거래만 포함하는 OTPB 방식을 적용하여 1,457 TPS의 처리속도를 낼 수 있게 됨으로써 비즈니스 거래에 적합한 방식임을 확인하였다. 제 5장 결론에서 블록체인을 쿼리 가능한 RDB에 적용했을 때 처리속도가 빨라지고 파일 크기가 축소되며 채굴 자동화 및 마켓 보상을 통해 오픈마켓에 적합한 모델이 될 수 있음을 확인하였다.

II. 블록체인을 공개마켓에 적용하기 위한 분석

비트코인 등 암호화폐의 근간이 되는 블록체인의 주요 기술인 분산원장, 암호화, 합의, 스마트 컨트랙트의 중요성을 인식하고 블록체인 기반 시스템 및 생태계를 조성하려는 움직임이 국내외에서 활발하게 진행되고 있다. 본 논문은 기존의 블록체인의 문제점과 대형 공개마켓의 문제점을 분석하고 블록체인 기술을 소형 공개마켓의 노드에 적용함으로써 소수에 의해 독점되지 않는 새로운 형태의 공개마켓 구현을 목표로 하였다.

2.1 블록체인

2.1.1 국내 동향

1) 16개 은행과 20여개 증권사가 '금융권 공동 블록체인 컨소시엄'을 구성하여 전자금융거래를 위한 고객인증, 위. 변조 여부 검증, 금융투자상품의

청산결제 업무 등 다양한 자동화 서비스 개발 진행[5].

2) LG CNS, SK C&C, Samsung SDS에서 물류 사업에 적용하기 위한 자체 블록체인 개발[5].

3) 과학기술정보통신부는 국내 블록체인 초기시장 형성과 글로벌 기술경쟁력 확보를 위한 '블록체인 기술 발전전략' 발표와 4차 산업 핵심 기술인 블록체인 활용 가능성 검증을 위한 여러 시범 사업 추진 공표[6][7]. 선거관리위원회는 전자투표시스템, 외교부는 블록체인 기반의 전자문서발급인증시스템, 농식품부는 축산물이력관리시스템, 국토부는 스마트 계약기반 부동산거래 플랫폼, 관세청은 스마트 개인통관 서비스 등 정부 주도의 블록체인 활성화가 진행되고 있다[5].

2.1.2 국외 동향

1) EU의 블록체인 활용 방안 심층 보고서[8].

2) 온라인 전자투표, 공문서 진위 판별, 제품 이력 추적, 디지털 미디어 저작권 관리, 지적 재산권 보호, 복지 및 의료 서비스 등 블록체인 활용 방안이 마련되고 있다[5][9][10].

2.2 공개마켓

온라인 쇼핑몰은 개인몰, 종합몰, 공개마켓, 소셜커머스로 나눌 수 있다. 공개마켓은 운영주체가 상품을 판매하지 않고 단지 장소를 제공하는 역할을 한다. 판매자는 경쟁적으로 싼 가격을 소비자에게 제공해야 살아남을 수 있기 때문에 지나친 가격 경쟁을 피할 수 없고 지불해야 할 수수료 부담도 크다.

공개마켓 조사에서 발견된 문제점 개선을 위해 블록체인에 적용했을 때의 장점은 다음과 같다.

1) 적은 수수료 부담

블록체인유지에 기여하고 있는 노드 참여자에게 1.0% 이하의 수수료를 지급하므로 공개마켓 운영자에게 판매액의 10%를 수수료를 지급하는 것에 비해 저렴하다.

2) 짧은 정산 주기

주문거래에 의해 파생한 복수의 상품거래를 각각의 계약으로 보고 주문거래에 속한 복수의 상품거래 계약을 하나의 블록에 묶어 봉인한 후 상품거래 계약에 대한 이행거래가 발생하면 에스크로 계정에 예치된 상품대금을 판매자에게 지불하는 방식이므로 계약 이행 즉시 정산된다.

3) 회원가입의 단순화

단순히 공개마켓 사이트 방문만 하는 고객을 위해 개인 정보 입력 없이 이메일 주소만 사용하여 회원가입이 가능하게 하고, 주문 거래가 발생한 때나 판매자로 전환할 때 필요 항목을 추가 등록하여 참여자의 정보 노출 부담을 최소화 한다.

4) 왜곡 없는 신용도

구매자가 상품을 선택하는 우선 순위는 판매자의 신용도와 상품평이 큰 비중을 차지하는데 중앙집중형 공개마켓의 경우는 운영자 또는 판매자에 의해 신용평가점수 및 상품평이 조작될 수 있다. 또한 상품 진열순서, 관련상품 등록 등 다양한 부분에서 공개마켓 운영자의 지배를 받게 된다. 상품거래와 상품평을 블록체인에 적용하면 실제 구매한 상품거래와 상품평이 유지되므로 운영자 또는 판매자가 신용도를 왜곡시킬 수 없다.

5) 완전 분산 마켓

참여 노드는 각자 도메인을 보유하고 해당 도메인은 마켓으로 운영된다. 회원 등록과 상품등록은 각각의 노드에서 하고 P2P 네트워크로 전파되어 공유한다. 주문과 정산은 에스크로 계정을 통해 자동 이행되므로 별도의 정산 관리자를 필요로 하지 않는다. 분쟁이 발생한 경우 각각의 노드에서 접수하고 P2P 네트워크로 전파되어 판매자에게 전달된다.

2.3 블록체인의 한계와 개선 방안

2.3.1 블록체인의 문제점

1) 채굴

비트코인은 목표 값보다 낮은 값이 나올 때까지 블록 헤더의 해쉬 작업을 무한정 반복하는 것이다. 채굴은 여러 참여자가 블록 생성에 기여하는 것이 아니라 대규모 자본을 투자한 재력가들의 사업으로 변질되었고 중앙 집중화된 채굴풀(Mining pool)에

의존하여 참여하기도 한다.

탈중앙화된 분산 시스템을 목표로 하였던 블록체인은 보상을 더 많이 차지하려는 특정인에 의해 채굴이 독점되고 중앙화되고 있는 문제점이 있다.

2) 처리시간

블록체인의 처리 속도는 TPS(Transaction Per Second)로 말하는데 비트코인은 7TPS, 이더리움은 10~30TPS, 비자(Visa)는 1,700TPS를 처리한다. 또한 블록 생성 권한을 얻기 위해 반복적인 블록 해쉬 값을 계산해야 하고 수신 된 거래들을 임시 풀에 거래들을 쌓아 놓았다가 블록 생성 권한을 얻게 된 때 수수료가 큰 것을 우선 선택하고 오래 대기한 거래를 순차적으로 선택하여 블록에 포함시키는 과정을 거친다. 그러나 공개마켓에서는 주문 거래를 쌓아놓지 않고 즉시 처리할 수 있어야 하고 더 빠른 처리 속도가 요구된다.

3) 확장성

비트코인의 경우 블록 생성이 10분에 1MB씩 증가하므로 년간 최대 52GB 증가하게 된다. 모든 노드가 전체 블록체인을 보관해야 한다면 100TB에 육박하게 되고 결국은 소수의 노드 참여자만 이를 감당할 수 있게 된다. 전체 블록이 커져서 소수의 노드만 전체 블록체인의 내역을 갖게 된다면 소수의 참여자가 결탁하여 블록 내용을 수정하는 등 조작행위가 일어날 수 있게 되는 문제점이 있다.

4) 포크 발생

블록 해쉬 값을 조건에 맞게 구한 채굴자가 여러 명일 경우 각자는 자신이 계산한 블록 해쉬 값으로 거래를 블록에 포함시킨 후 블록체인에 추가하고 P2P 네트워크로 전파한다. 이때 또 다른 노드가 동일한 방식으로 블록을 전파하게 되면 두 개의 블록체인은 모두 정당하다. 또 다시 새로운 블록을 추가할 때는 두 개의 서로 다른 블록 중 가장 긴 체인을 옳은 것으로 간주하여 그 체인이 계속 확장하도록 작업을 수행한다[1].

III. 거래와 블록 구성 방법 설계 (ACABD 블록체인)

3.1 거래와 블록에 OTPB 적용

본 논문의 목표는 중앙 집중형 공개마켓과 달리 분산형 공개마켓 플레이스에서 운영자의 개입 없이 계약과 이행이 자동 처리되는 블록체인을 적용하는 것이다. ACABD 블록체인에서 거래로 다뤄지는 것은 화폐, 게시물, 계약이다.

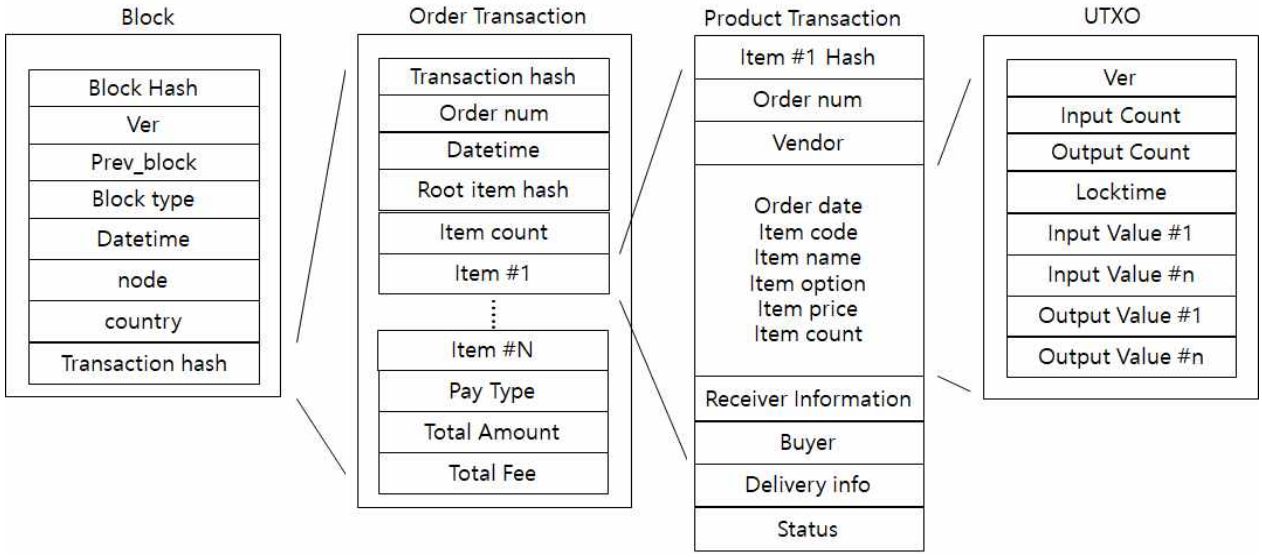

그림 4. ACABD 거래 블록
Fig. 4. ACABD transaction block

ACABD 블록체인에서 블록은 화폐, 게시물, 계약 등 세 가지 유형으로 구분한다. 화폐는 블록체인에서 정산할 때 필요하며 공개마켓 플레이스 환경에서만 사용 가능하다. 게시물은 상품평과 하자처리로 나뉜다. 계약은 상품등록과 주문거래 및 상품거래, 배송거래로 구분한다. 상품등록은 반복적으로 사용하는 일반 상품과 한번 구매하면 소멸되는 일회성 상품으로 구분되며 주문거래는 상품거래를 수반하고 배송거래는 상품거래에 대한 이행과정이다. 배송거래가 완료된 때 정산이 개시된다.

그림 4에서와 같이 ACABD 블록체인에서는 블록은 한 개의 주문거래이며 여러 개의 상품거래(Items)를 포함하고 있다. 상품평의 경우에도 동일한 블록 구조가 적용된다.

1) 상품평 거래 생성

상품 정보가 홍수를 이루면서 구매자는 신뢰할 수 있는 일부 브랜드를 제외하고는 상품을 기억하지 않는다. 상품을 구매할 때는 온갖 정보를 들여다보고 비교하는 정보 수집과정을 거쳐 구매를 결정하고 이후에는 상품 리뷰를 통해 사용 경험을 공유하는 과정을 반복한다. 구매 의사결정에 가장 큰 영향을 주는 것은 상품리뷰이며 본 논문에서는 이 부분 역시 블록체인을 적용하여 상품평이 왜곡되지 않도록 구현하였다.

2) 주문거래와 상품거래

본 논문에서는 계약을 주문거래와 상품거래로 구분하였다. 주문거래는 구매자가 상품을 카트에 넣고 최종 구매를 결정한 때에 발생한다. 상품거래는 하나의 상품(item)일 때와 여러 상품(items)일 때가 있고 한 판매자(vendor) 또는 여러 판매자(vendors) 일 수 있으며 여러 상품일 경우에도 한 판매자일 수 있다.

3) 거래 상태 및 이행 확인

비트코인에서 UTXO는 아직 사용하지 않은 화폐의 합을 의미한다. 본 논문에서 UTXO는 비트코인과는 달리 한 개의 주문거래에서 발생한 여러 상품거래가 배송 결과로 계약이 이행되는 과정에 존재하며 배송이 완료되면 정산 절차를 개시토록 한 후 소멸한다. 즉 본 논문에서 UTXO는 계약이행이 남아 있는 상태의 합을 말한다.

3.2 ACAB블록 생성

1) ACABD 블록체인의 블록 헤더

ACABD 블록체인에서 블록 헤더는 8개 항목으로 구성되어 있다. Block Hash는 ver, prev_block, block_type, time, node, country, tran_hash 등 7개 항목을 이어 붙힌 값에다 SHA256 해시를 이중으로 적용하고 값을 뒤집은 결과 값이다. 블록 해쉬 값 계산은 그림 5와 같은 7단계를 거친다.

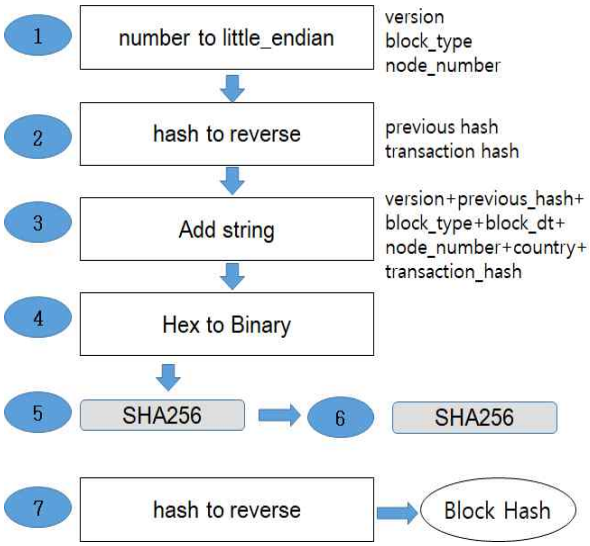

그림 5. ACABD 블록 해쉬 값 계산 절차
Fig. 5. ACABD block hash value calculation procedure

2) 트랜잭션과 해시

본 논문에서 사용하는 주된 트랜잭션은 주문거래, 게시물, 상품등록이다. 트랜잭션은 block_type 에 의해 구분되며 블록헤더에 각 2, 3, 4로 표시되고 OTPB 방식에 의해 하나의 블록에 하나의 주된 트랜잭션이 기록 된다. 주된 트랜잭션의 해쉬 값 계산 대상은 화폐거래,주문거래,상품등록,게시물이다.

주문거래의 해시 값은 식 (1)과 같이 구한다. Item Root 해시 값은 머클트리 방식을 사용한다.

$$H = \text{Block\_type}(1) + \text{Order\_num}(20) + \text{Datetime}(8) + \text{Item Root}(32) \quad (1)$$

게시물은 블록체인에서 허용할 최대 게시물의 개수를 미리 정하고 게시물이 블록으로 만들어 질 때마다 Thread 값을 순차적으로 줄여 나가는 방법을 사용한다. 블록체인에서 특정 게시물의 하위 게시물이 발생할 경우, 원래 게시물의 Thread 값을 기록하여 종속 관계를 갖도록 한다.

3.3 합의와 채굴 자동화

비트코인은 블록 처리시간이 7 TPS 이고 블록 생성 간격이 10분이므로 수많은 거래가 발생하게 되면 임시 풀에 저장하고 수수료가 많거나 저장이 오래된 순서에 의해 선택적으로 새로운 블록에 포함되고 P2P 네트워크로 전파되어 6회 이상의 확인을 받아야만 유효한 거래로 인정된다[4]. 공개마켓 플레이스에서는 주문거래가 많고 결제 과정은 신속해야 하기 때문에 임시 풀에 저장된 후 선택적으로 블록에 포함돼서는 안된다. ACABD 블록체인은 자신의 노드를 제외한 모든 노드의 최종 블록에 대한 위.변조를 검사하는 합의과정과 새로운 블록 해쉬 값을 자동 생성하는 ACAB 방식을 적용하였다.

ACAB방식은 주문거래가 발생한 노드에서 마지막 블록을 읽어 직전 블록의 해시 값과 새 블록에 사용할 순차 값을 구한 후 다른 요소와 합쳐 새로운 블록 해시 값을 계산한 후 블록을 생성하며, 인증서버에 기록된 다른 노드의 IP를 이용하여 순차적으로 원격 접속하고 동일한 방법으로 직전 블록의 왜곡여부를 확인한 후 새로운 블록을 자동으로 추가한다. 이러한 방식은 노드에 의해 반복적으로 블록 해쉬 값을 구하여 블록 생성 권한과 화폐 보상을 받는 채굴 기능을 제거함으로써 과도한 채굴 경쟁과 비용 낭비를 제거하고 실시간으로 거래를 블록에 포함시킴으로써 처리시간을 단축시킨다.

IV. 공개마켓에서 ACABD 블록체인 구현

특화된 분야(예. 잉여자재 공개마켓)에 적용가능한 소규모 공개마켓을 설계하고 누구나 구매자와 판매자가 될 수 있는 환경을 구축한다. 회원가입은 개인정보를 사용하지 않는다. 공개마켓에 적용되는 블록은 화폐, 게시물, 계약 등 세 가지로 구분되며 계약은 상품등록, 주문, 상품거래로 세분된다. 주문 계약이 완료되고 정산이 개시될 때 상품거래 마다 UTXO를 생성하여 판매자 및 거래에 기여한 노드에게 보상으로 전자지갑 주소에 전송한다. 계약에 해당 하는 주문거래 및 상품거래는 결제가 완료되면 임시 풀에 머물지 않고 즉시 블록이 생성되고 블록체인에 추가되며 노드들에게 전파된다.

4.1 인증 서버

1) 노드

노드 도메인은 마켓 운영과 P2P 네트워크 주소로 사용된다. 공개키는 수수료를 보상할 때 상대방이 노드의 전자지갑 주소로 UTXO를 생성한다.

2) 참가자

개인을 식별할 수 있는 정보를 요구하지 않고 단순하게 이메일, 회원명, 비밀번호만으로 회원가입을 한다. 회원 가입이 되면 개인키가 생성되고 개인키를 이용하여 공개키와 전자지갑 주소가 생성된다. 개인키는 가입자가 보관하는 것을 원칙으로 한다. 상품 구매를 위한 참여자는 노드가 운영하는 공개마켓에 접속하여 로그인하고 상품주문과 결제를 한다.

4.2 상품 등록

ACABD블록체인 기반의 공개마켓은 모든 노드가 독립적으로 마켓을 운영할 수 있으므로 상품 등록을 블록체인에 적용할 때 자신이 등록한 상품인지 다른 노드로부터 P2P 네트워크로 전파된 상품인지 구분하도록 한다. 상품 유형은 서비스 및 용역, 중고물품과 같이 상품이 판매됨과 동시에 소멸하는 일회성 상품과 한 번 등록하면 반복적으로 판매할 수 있는 일반 상품이 있다. 기존의 블록체인을 이용하여 상품을 등록한다면 1~4Mb 용량 제한에 걸린다. ACABD 블록체인은 데이터베이스의 BLOB 속성을 이용하여 상품 이미지를 저장할 수 있으므로 이미지를 많이 사용하는 공개마켓에 적합하다.

상품정보에 사용되는 이미지를 블록에 저장할 때, 이미지 파일에 포함된 예기치 않은 특수문자를 제거하기 위해 chunk_split 함수와 base64_encode 함수를 사용하였다.

$img = chung_split(base64_encode(file_get_contents ($tmpfile)));
이미지를 꺼내 보려면 base64 디코딩을 거친 후 img tag를 사용한다.
$img= base64_decode(img)
<imgsrc=$img>

4.3 주문거래와 상품 묶음 관리

상품 #1의 해쉬 값은 Item Hash로 묶어준 Order_num, Sequence, 주문상품정보 등 세 항목을 연결하여 계산하고 주문거래에 상품 #1로 저장시킨다. 상품 #n까지 해쉬 값을 계산하여 순차적으로 주문거래에 저장하였으면 다시 이들 상품 #1 부터 상품 #n까지를 연결하여 Root Item Hash 값을 계산한 후 저장한다.

Root Item hash = hash('sha256',Item #1 + Item #2 + Item #3 + Item #n) (2)

상품거래에서 상품 #1 부터 상품 #n까지 반복되므로 연관 배열로 만든 후 다시 JSON Format으로 변환하여 평문(plain text)을 만들어 블록에 저장한다.

한 개의 주문거래에 속한 상품거래는 Order_num으로 종속관계를 가지며 개별 상품마다 판매자가 다를 수 있다. 판매자가 다른 경우 수령인에 대한 정보를 상품마다 제공해야 한다.

4.4 판매 보상

비트코인의 경우 채굴을 하면 화폐로 보상을 해준다. 그런데 처음부터 2,100만 비트코인이 발행되도록 설계되었기 때문에 채굴이 고갈된 이후에 채굴자들이 인센티브 없이 계속 네트워크를 유지해 줄 것인가 하는 의문이 있다[11].

ACABD 블록체인은 거래가 발생하면 OTPB 방식에 의해 한 개의 블록이 생성된다. 블록 해쉬 값은 자동 계산되고 인증 서버를 이용하여 자신을 제외한 모든 노드의 직전 블록 해쉬 값을 비교하여 합의 과정을 거치므로 채굴자가 필요하지 않고 채굴에 따른 보상도 없다.

ACABD 블록체인은 모든 노드가 마켓을 유지하는 공개마켓 플레이스 환경을 제공하기 때문에 구매자가 블록체인을 검색하여 상품을 선택하고 결제할 때 판매자는 상품판매 수익을 얻게 된다. ACABD 블록체인의 보상은 판매금액의 1% 를 기본 적용한다. 중앙 집중형 공개마켓 수수료의 1/10에 해당하지만 참여 노드와 구매자가 증가할수록 수수료 규모는 커진다. 판매자가 상품을 등록할 때 기본 수수료 보다 더 많은 수수료를 제공할 경우 노드가 운영하는 마켓은 더 많은 보상을 받기 위해 해당 상품을 많이 노출시킬 것이다.

주문거래가 발생하면 결제대금은 에스크로 계정에 보내지고 배송이 완료되면 개별 상품마다 다음과 같이 네 개의 UTXO가 생성되어 정산절차가 진행된다.

- 물품대금 UTXO : 판매대금에서 보상(수수료)를 공제한 금액
- 마켓보상 UTXO : 구매자가 접속하여 상품주문을 한 마켓 보상
- 회원보상 UTXO : 구매자를 가입시킨 노드에 대한 회원 보상
- 공급보상 UTXO :판매자를 가입시킨 노드에 대한 공급 보상

완전한 공개마켓에서 노드는 마켓 역할을 하고, 각 노드는 자신에게 회원 등록된 구매자와 판매자가 있다. 이런 조건은 모든 노드의 조건과 같다. 구매자는 자신이 가입한 노드의 마켓을 이용할 수 있고 다른 마켓을 이용할 수도 있다. 구매자는 자신이 가입한 노드의 마켓에 상품을 판매하는 판매자의 상품을 구매할 수도 있고 다른 마켓에서 등록한 상품이 블록체인으로 공유되어 구매하는 경우도 있다.

물품대금을 정산 할 때 판매자에게 지급하고 남은 수수료는 마켓, 판매자, 구매자의 조건에 따라 UTXO를 생성하여 전자지갑에 전송한다.

4.5 시뮬레이션

실험은 블록 헤더를 DB에 체인으로 추가하는 과정에서 매 건마다 직전 생성된 블록의 위.변조 여부

를 점검하는 “합의”와 새로 추가될 블록의 해쉬 값을 계산하여 블록 헤더를 완성하고 체인에 추가하는 과정을 2,000,000번 수행하였다. 쿼리가 지원되는 RDB 방식을 블록체인에 적용하였을 때 기존의 DB4 방식에 비해 어떤 차이가 있는가를 비교하는 것이므로 네트워크 상태에 따른 전송속도의 차이점을 배제하였고 단일 노드에서의 동일 조건의 블록을 생성하였다. 동일한 조건으로 비트코인에서 사용되고 있는 Berkeley DB 4.8.30에 블록 데이터를 생성하고 처리속도와 파일 사이즈를 비교하였다.

블록은 다음과 같은 데이터로 구성하였다.

```
$input['block_hash'] = $new_code;
$input['ver'] = $ver;
$input['prev_block'] = $prev_block;
$input['block_type'] = $block_type;
$input['block_dt'] = $block_dt;
$input['node_num'] = $node_num;
$input['country'] = $country;
$input['tr_hash'] = $tr_hash
```

ACABD 블록체인 기반의 공개마켓은 웹 환경에서 클라이언트에서 웹 브라우저로 연결하여 테스트하였다. 이때 응답시간과 대기시간은 통신 환경에 따라 달라질 수 있기 때문에 공정한 테스트를 위하여 동시 사용자 없이 단독으로 클라이언트와 서버가 접속되고 RDB 및 DB4가 연결된 상태까지는 시간을 측정하지 않았다. 또한 호출간격은 따로 제한하지 않고 처리 대상이 완료될 때까지 반복적으로 작업하였다.

10만건 단위로 20번 나누어 처리시간(초), CPU사용률, 메모리 사용량, 메모리 Peak 사용량(Kb)을 측정하였는데 CPU 사용량과 메모리 사용량은 모든 테스트에서 동일하거나 경미하여 분석 대상에서 제외하고 처리시간과 메모리 Peck 사용량을 대상으로 비교하였다. 10만 건 단위로 DB 연결과 Open 및 Commit을 수행하였다. DB4의 경우에도 10만 건 단위로 DB handler와 File을 Open 및 Close 하며 수행하였다. 블록 헤더를 구성할 때 사용된 거래명세 해시는 따로 계산하지 않고 한 개의 고정 값을 구한 후 블록 헤더를 생성할 때 마다 동일한 해쉬 값을 사용하였다. 측정 방법은 직전 블록을 검사하고 새로운 블록의 해쉬 값을 계산하여 순차적으로 블록을 추가하는 과정을 200만번 수행하였고 생성된 블록을 랜덤 검색하는 실험을 하였다.

블록 생성 속도는 MySQL(이하 RDB라 한다)에서는 10만건 당 68.61 sec, Berkeley DB(이하 DB4라고 한다) 에서는 104.22 sec 소요되었다.

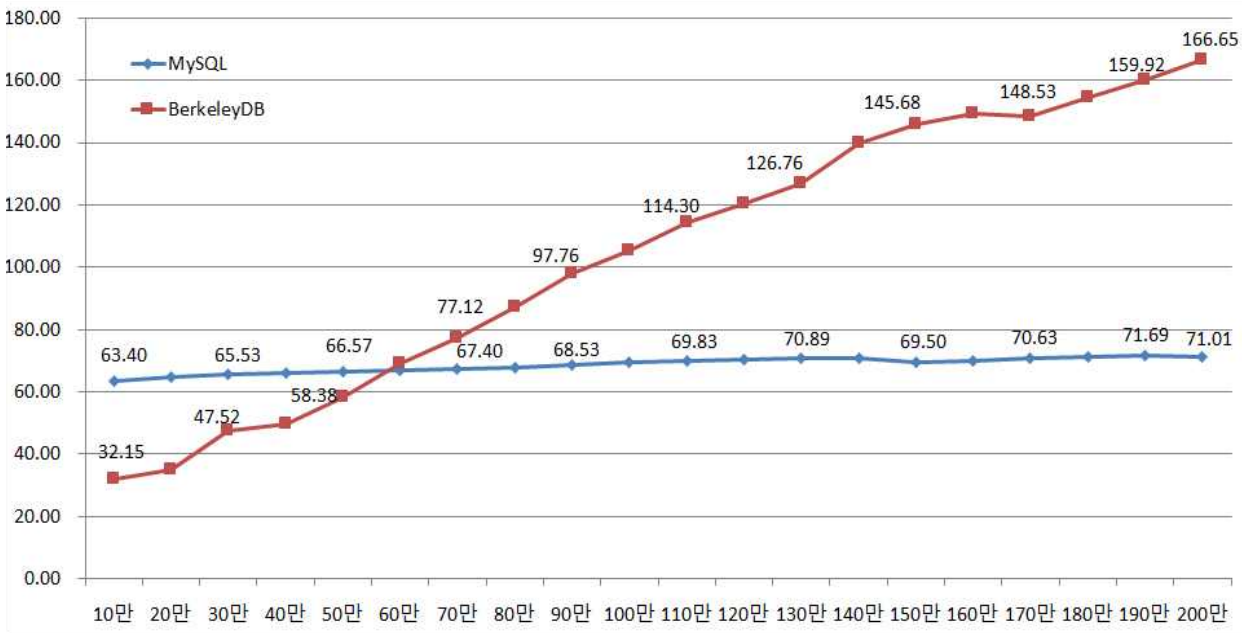

그림 6. 블록헤더 생성 처리 측정 결과 비교

Fig. 6. Block header generation processing measurement result comparison

그림 6을 보면 블록 개수가 적을 때 10만 개 당 DB4가 RDB에 비해 2배 빠른 처리 속도를 보였는데 60만개를 처리할 때는 DB4는 68.89초, RDB는 66.93초로 역전되었으며 200만개를 처리할 때는 DB4는 166.65초, RDB는 71.01초의 처리 속도를 보였다. DB4는 데이터가 적을 때 32.15초가 걸렸지만 200만 건을 처리할 때는 5배가 느려진 166.65초가 걸렸다.

비트코인의 블록 사이즈는 약 1MB로 고정되어 있고 블록 생성시간은 약 10분이므로 초당 처리할 수 있는 사이즈는 약 1.71KB가 된다.

$$1.71Kb = 1,024Kb / 600sec \quad (3)$$

이더리움의 블록 사이즈는 약 30KB이며 블록 생성 시간은 약 10~20초이므로 초당 처리할 수 있는 사이즈는 2KB가 된다. 이더리움이 비트코인에 비해 블록생성시간이 짧지만 초당 처리능력은 비슷하다.

$$2Kb = 30Kb / 15sec \quad (4)$$

ACABD 블록체인은 RDB에 기록하는 처리시간을 측정해 본 결과 네트워크를 제한 속도를 고려하지 않았을 때 1,457 TPS가 측정되었다. 이러한 속도는 공개마켓에서 실시간 거래를 처리하는데 문제가 될 것이 없다.

그림 7을 보면 RDB의 파일 사이즈는 데이터 부분과 인덱스 부분을 합해 359.97Mb, DB4의 경우는 721.44 Mb로써 두 배가 크다는 점이다. 200만개의 블록을 생성했을 때 RDB는 719.81Mb, DB4는 1,444.28 Mb를 보여주었다.

그림 8을 보면 순차 검색의 경우에는 메모리 사용량이 RDB와 DB4가 비슷하게 사용되고 있지만 랜덤 검색의 경우에는 DB4가 많은 메모리를 사용하고 있다.

본 논문에서 기존 블록체인 방식의 DB4와 새로운 비즈니스 모델에 적합한 RDB 방식을 비교했을 때 데이터가 적을 때는 DB4가 빠르지만 데이터가 많아지면 RDB가 4배 이상 빠르다는 것을 확인하였다. 블록 200만건 생성에서 60만 건을 교차점으로 RDB가 DB4 보다 빠른 블록체인을 생성하는 것이 확인 되었으며 데이터 처리 전체 구간에서 RDB는 균등한 속도를 유지되는 안정성도 확인되었다.

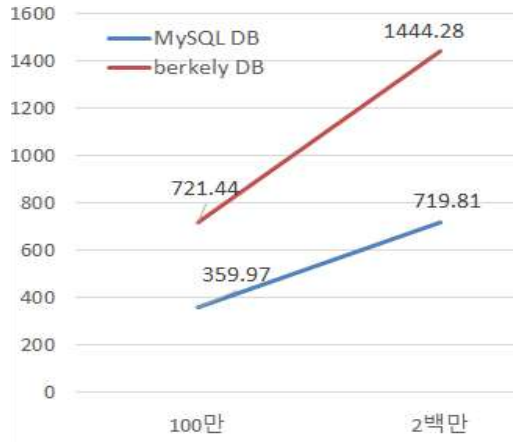

그림 7. 블록체인 사이즈 비교
Fig. 7. Blockchain size comparison

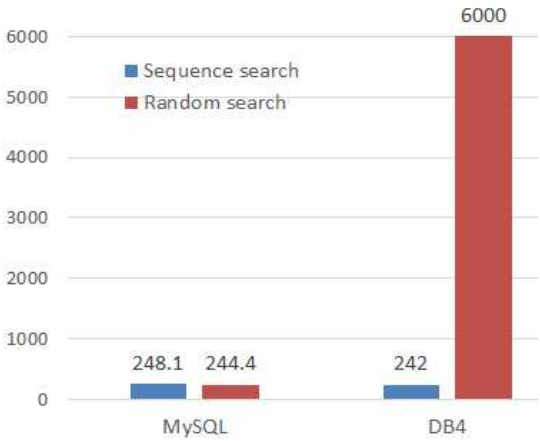

그림 8. 순차 및 랜덤 검색 메모리 사용량 비교
Fig. 8. Sequence and random search memory usage comparison

V. 결론 및 향후 과제

본 논문에서 제안한 ACAB 알고리즘은 트랜잭션이 발생한 마켓에서 자신의 인증 서버를 통해 블록을 생성하고 브로드케스팅 함으로써 채굴자에 의한 채굴과정을 제거하는 모델을 제시하였다.

동일한 조건으로 RDB와 DB4에서 블록 생성 실험을 했을 때 RDB는 190만 건 상태에서 10만 건을 추가할 때 71.01초, DB4는 190만건 상태에서 166.65초 걸렸다. 블록체인의 크기가 커져도 RDB는 일정 처리 속도를 유지한 반면 DB4는 급격히 처리 속도가 늦어졌다. 파일크기는 RDB가 719.81Mb, DB4는 1,444.28Mb 였다. 랜덤검색에서 RDB는 일정한 메모리를 사용했지만 DB4는 메모리 사용량이 늘어났다. 본 논문에서 제안한 OTPB 알고리즘과 ACAB 알고

리즘은 거래 즉시 블록 해쉬 값을 자동 계산해 주기 때문에 RDB 기반의 블록체인이 비즈니스 모델에 적합하다. 쿼리가 지원되는 RDB 형태의 블록체인에 상품평 등 신뢰할 수 있는 빅데이터가 구축되면 AI Chatbot을 이용한 고객의 요구사항을 자동화할 수 있다.

향후 연구과제는 첫째, ACABD 블록체인의 보상이 마켓보상, 회원보상, 공급보상으로 되어있는데 모든 노드가 동등하므로 새 노드가 추가될 때 블록체인 DB를 백업하여 데이터를 제공하는 노드에게 보상을 제공하기 위한 업무량 측정과 보상비율을 결정해야 하는 일이다. 둘째, 마켓과 RPC 모듈의 버전 관리와 업그레이드의 주체를 모든 노드에게 공개하고 공유했을 때 ACABD 블록이 왜곡되지 않고 지속될 수 있는 방법을 찾는 것이다.

References

[1] S. Nakamoto, "Bitcoin:A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf, Oct. 2008. [accessed: Sep. 20, 2019]

[2] M. Ripeanu, "Peer-to-peer architecture case study: Gnutella network", Proceedings First International Conference on Peer-to-Peer Computing, Linkoping, Sweden, pp. 99-100, Aug. 2002

[3] Hee-Bog Kang. Haeng-Cheon Jang, and Chang-Soo Jang, "IUWT Based Token Authentication Technology", Journal of KIIT, Vol 17. No. 2, pp. 143-150, Feb. 2019

[4] EKokorisKogias, P Jovanovic, N Gailly, I Khoffi, L Gasser, and Bryan Ford, "Enhancing Bitcoin security and performance with strong consistency via collective signing", 25thUsenixSecurity, 2016.

[5] National IT Industry Promotion Agency, "Blockchain Industry Status and Trend", NIPA, Issue Report 2018-17, 2018.

[6] Ministry of Science and ICT, "Blockchain Technology Development Strategies for a Reliable Fourth Industrial Revolution", MSIT, 2018.

[7] Gyeonggi Research Institute, "Suggestions for Building Blockchain-based Public Platforms", Issue & Diagnosis, 328, 2018.

[8] P.Boucher, S.Nascimento, M.Kritikos, "How blockchain technology could change our lives: In-depth Analysis", European Parliamentrary Research Service, 2017

[9] "EU Blockchain Observatory and Forum", www.eublockchainforum.eu, appect : 2019-08-13. [accessed: Sep. 20, 2019]

[10] MyungSan Jun, "Blockchain government –a next form of infrastructure for the twenty-first century", Journal of Open Innovation: Technology, Market and Complexity, Vol. 4, Article No. 7, pp. 1-12, Feb. 2018.

[11] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayanan, "On the Instability of Bit-coin Without the Block Reward", Proceedings of the 2016 ACM SIGSAC Conference on CCS, Vienna Austria, pp. 154-267, Oct. 2016.

저자소개

강 희 복 (Hee-Bog Kang)

2015년 2월 : 전남대학교 컴퓨터공학과(공학석사)
2020년 1월 : 전남대학교 컴퓨터공학과(공학박사)
2020년 4월 ~ 현재 : ㈜샘이깊은물 개발이사
관심분야 : 컴퓨터네트워크, 클러스터링, 웹서비스, 블록체인, 챗봇

장 창 수 (Chang-Soo Jang)

1980년 2월 : 조선대학교 전자공학과(공학사)
1982년 8월 : 건국대학교 전자공학과(공학석사)
1997년 2월 : 서강대학교 컴퓨터공학과(공학박사)
1984년 ~ 현재 : 전남대학교 컴퓨터공학과 교수
관심분야 : 병렬처리구조, 컴퓨터네트워크, DSP