논문 21-46-01-13 The Journal of Korean Institute of Communications and Information Sciences '21-01 Vol.46 No.01
https://doi.org/10.7840/kics.2021.46.1.102

5G 기반 서비스 제공에 적합한, 실시간성을 갖는 블록체인 구조 제안

이 승 호◆, 김 기 천°

Proposal of Blockchain Structure with Real-Time Capability Suitable for 5G-Based Service Provision

Seungho Lee◆, Keecheon Kim°

요 약

5G와 사물인터넷을 기반으로 한 서비스 상용화를 위한 난관 중 한 가지로 보안 취약점이 있다. 이를 해결하기 위한 다양한 연구가 진행되고 있으며 블록체인 역시 유력한 대안 중 하나로 연구되고 있다. 하지만, 현재의 블록체인은 보안성만 보장할 수 있을 뿐 실시간 서비스 제공을 위한 처리 속도는 갖추지 못하고 있다. 따라서 요구되는 성능을 제공할 수 있는 새로운 블록체인 구조를 제안하고자 한다. 대표적인 블록체인들의 장단점을 분석해 보안과 성능 두 가지를 모두 제공하는 데 있어 문제 되는 요소들을 추려내었다. 이 중 블록체인의 무결성을 보장하는 동시 프라이버시가 보장되지 못하는 양날의 검이면서, 중복 거래 등을 방지하기 위해 빠른 블록 전파가 요구되어야 하는 공동 장부를 개선하는 방안을 제안한다. 본 논문은 개선된 장부와 PoB 기반 합의 알고리즘, 스마트 계약의 CA를 활용한 인증구조를 통해 기존의 보안성을 유지한다. 또한, 개인장부와 peer 네트워크를 통해 네트워크를 간소화하고, 제안한 PoB 기반 알고리즘으로 경쟁형태의 합의로 인한 자원낭비 및 네트워크 과부하를 해소한다. 위와 같은 기술적인 근거를 통해 실시간 서비스 제공을 위한 처리를 수행할 수 있음을 증명하였다.

키워드 : 사물인터넷, 블록체인, 분산원장, 머클 트리, 신뢰 기반 증명
Key Words : IoT, Blockchain, Distributed Ledger, Merkle Tree, PoB

ABSTRACT

Security vulnerabilities are one of the difficulties in commercializing services based on 5G and IoT. Various studies are being conducted to solve this problem, and blockchain is being studied as one of the promising alternatives. However, the current blockchain can only guarantee security and doesn't have a processing speed for providing real-time services. So, we'd like to propose a new blockchain structure that can provide the required performance. By analyzing the pros and cons of representative blockchains, we have identified the problematic elements in providing both security and performance. Among them, we propose a method to improve the Shared Ledger, which is a double-edged sword that guarantees the integrity and doesn't privacy at the same time, and requires rapid block propagation to prevent duplicate transactions. This paper maintains security through the improved ledger, PoB-based consensus algorithm and the authentication structure using the

※ 본 연구는 2020년도 국토교통부/국토교통과학기술진흥원(20TLRP-B152768-02)의 지원과 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단(2020R1A2C1101392)의 지원을 받아 수행되었습니다.
◆ First Author : Konkuk University Department of Computer Engineering, phg0726@konkuk.ac.kr, 학생(석사), 학생회원
° Corresponding Author : Konkuk University Department of Computer Engineering, kckim@konkuk.ac.kr, 정교수, 종신회원
논문번호 : 202010-247-C-RN, Received October 5, 2020; Revised November 2, 2020; Accepted November 4, 2020

CA of smart contracts. In addition, the network is simplified through personal ledger and peer networks, and the proposed PoB-based algorithm is used to eliminate waste of resource and network overload due to agreement of competitive form. The above technical rationale has demonstrated that processing for real-time service delivery can be performed.

Ⅰ. 서 론

최근 5G 통신기술의 발전과 함께 모든 사물이 네트워크로 연결되는 사물인터넷(Internet of Things, IoT)이 주목받고 있다. IoT는 각종 사물에 내장된 센서를 통해 수많은 정보를 수집하며, 무선통신기술을 통해 네트워크에 연결한다.

수많은 IoT 기기들을 네트워크 내에 수용하고 관리하는 것은 시스템 입장에서 매우 어려운 일이지만, 무선 통신기술의 발전에 따라 5G에서는 광대역 무선 통신 eMBB(enhanced Mobile Broad Band), 안정성 및 지연시간 최소화를 위한 URLLC (Ultra-Reliable Low Latency Communication) 기술, 대규모 기기 연결 mMTC(massive Machine-Type Communication)을 통해 밀도 높은 연결기기 들에 대해 서비스를 제공한다[1].

반면, 보안에 있어 IoT는 여전히 취약하다. IoT는 센서/장치, 게이트웨이와 같은 다양한 물리적 구성요소와 통신/네트워크 기술 그리고 서비스 API 기술 및 사용자 인터페이스 기술과 같은 다양한 기술 요소들을 포함하고 있으며 이를 통해 다양한 기기들에 대해 서비스를 제공한다. 하지만 이러한 연결은 각 구성요소에 없던 취약성이 유입되는 원인이 되었으며, 자원이 제한된 IoT 기기의 특성은 DDoS(Distributed Denial of Service) 공격에 취약할 수밖에 없다[2].

이러한 취약점을 해결하기 위한 여러 방면의 연구가 진행되고 있으며, 해결방안 중 하나로 블록체인 기술이 기대되고 있다.

블록체인의 특성을 이용해 IoT의 한계를 극복하는 연구[3]를 시작으로 새로운 합의 메커니즘을 개발하여 적용[4]하는 등 다양한 연구들은 실제로 IoT의 보안 취약점을 해결하는 결과를 내보이고 있다. 하지만 이러한 연구들은 대부분 사용 환경이 제한되어 있으며, 공용 가능한 솔루션들도 보안만을 강화할 뿐 실제로 IoT에 요구되는 실시간 서비스를 제공하는 데 있어 오히려 블록체인 내에서의 작업이 서비스 지연을 일으키는 요인이 되고 있다.

본 논문에서는 블록체인 적용을 통해 목표로 하는 보안성을 제공하면서도 실시간 서비스 제공에 악영향을 끼치지 않고자 한다. 이를 위해 기존 블록체인들을 분석하여 보안성, 실시간 서비스 양쪽 제공에 악영향을 끼치는 요소들을 분석하고 이를 바탕으로 한 새로운 블록체인 구조를 제안한다.

Ⅱ. 관련 연구

2.1 Blockchain

블록체인은 분산 원장 기술로 합의적으로 원장에 대한 공유, 복제, 동기화가 이루어지는 데이터베이스이다.

현재, 금융 거래는 은행과 같은 중앙 기관에 의존하고 있으며 해당 기관의 보증 하에 예금의 금액, 발신자, 날짜 및 시간 등 처리되어 주어지는 거래와 관련된 정보들을 신뢰한다. 즉, 중앙의 저장소에 의존하여 기록 수집 및 유지, 보호가 이루어지는 구조이다[5].

반면, 블록체인은 신뢰의 근간이 되는 저장소를 분산한다는 점에서 기존의 저장구조와 차이를 보인다.

[그림 1]과 같이 네트워크에 참여한 모든 참여자가 기록을 공유하는 구조로 신뢰할 수 있는 제삼자가 존재하지 않는 구조이다. 해당 구조는 언뜻 보기엔 중앙기관 없이 기존의 서비스 제공이 가능한 구조로 보이지만, 특정 참여자를 중심으로 한 단체가 정보를 위변조할 경우 네트워크 참여자 전체가 위조된 정보를 공유하게 될 가능성이 존재한다. 이를 방지하기 위해 존재하는 것이 '블록체인'이다.

블록체인은 말 그대로 여러 개의 블록이 체인의 형태를 이루고 있으며, 새로 생성되는 블록은 이전에 생성된 블록의 해시 값을 가지고 있다. 이 해시 값은 새

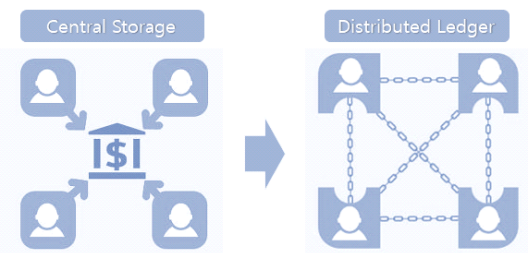

그림 1. 원장 기록 방식의 변화
Fig. 1. Changes in ledger recording methods

로 생성되는 블록의 해시 값 결정에 영향을 끼치는 요소 중 하나로 특정 거래 기록을 위변조할 경우 해당 기록을 포함하는 블록과 이 블록과 이어진 블록들의 해시 값 역시 바뀌게 된다. 때문에, 네트워크 참여자들은 공유된 기록들을 바탕으로 이러한 변화를 감지하고 조작된 정보의 공유를 막을 수 있다.

2.2 Bitcoin Analysis

비트코인은 블록체인 기술을 활용한 최초의 가상화폐이다. 블록체인의 분산장부, 체인 구조가 가진 특성을 그대로 계승하며, 처리된 트랜잭션들을 체인에 반영하기 위한 합의 프로세스는 PoW(Proof of Work)를 통해 이뤄진다. PoW는 흔히 '채굴'이라 불리는 방식으로 채굴자는 previous hash, merkle hash 등 블록 헤더 구성 값에 nonce라는 난수를 포함하여 블록체인이 지정한 난이도를 만족하는 해시 값을 찾는다. 해시 값을 찾은 채굴자는 해당 값을 네트워크를 통해 전파하며, 네트워크 참여자들로부터 과반수의 동의를 얻어내면 생성될 블록의 해시 값으로 지정된다. 해시 값을 찾은 채굴자는 체인에 블록이 등록되는 동시 보상으로 가상화폐를 받으며, 위와 같은 보상 구조로 합의 프로세스 참여를 유도한다[6].

하지만 PoW는 블록체인의 가장 큰 문제점이기도 하다. 채굴이라는 경쟁 형태의 합의 프로세스는 하나의 블록을 채굴하는 데 필요 이상의 자원이 소모된다. 또한, 과반수의 동의를 통해 블록 생성이 확정된다는 것은 반대로 해당 수의 동의를 얻기 전까진 블록 생성이 지연됨을 의미한다. 실제로 비트코인은 해당 요인과 채굴난이도를 포함하여 평균 10분의 간격으로 블록이 생성되며 초당 트랜잭션 처리 속도는 7tps로 실시간 처리가 요구되는 서비스 제공이 불가능하다[7].

분산장부 역시 문제점을 가지고 있다. 공유 및 동기화를 통해 공통의 장부를 소지함으로써 무결성을 가지지만 투명성으로 인해 프라이버시가 침해되기도 한다. 이를 방지하기 위해 익명을 통한 전달, 공개키를 이용한 한정적 접근 등 관련 연구[8]가 진행되고 있지만 실용화하기에는 PoW 과정에서 해시 계산으로 인한 지연, 접근 및 전파에 대한 예측 등 여러 문제점이 남아있다.

2.3 Ethereum Analysis

이더리움은 스마트 계약을 활용한 최초의 가상화폐이다. 스마트 계약이란 계약 지향 프로그래밍 언어 Solidity로 구성된 전자 계약으로 계약 이행 및 검증까지의 거래 프로세스가 자동화되어있다. 프로그래밍 언어를 활용함으로써 비트코인보다 블록체인에 기록할 수 있는 정보의 범위가 확장되었으며, 비교적 적은 비용으로 거래를 신속하게 처리할 수 있다. 게다가 gas라는 개념을 도입해 생성된 코드를 실행함에 따라 실행 비용이 발생토록 하고, gas limit를 통해 코드를 실행할 수 있는 횟수를 제한하여 DDoS(Distributed DoS)와 같이 자원 소모를 유도하는 공격에 대해 면역을 가진다.

이더리움은 스마트 계약을 활용하기 위해 두 가지 계정이 존재한다. 하나는 EOA(Externally Owned Account)로 사용자의 통제 하에 개인키를 관리하고 트랜잭션을 생성하는 계정이며, 다른 하나는 CA(Contract Account)로 트랜잭션과 연결된 계정이며, 계약 진행을 위한 트리거 역할을 한다.

[그림 2]과 같이 EOA가 특정 거래를 생성 후 CA로 ETH를 전송하고 입력된 조건을 충족하면 코드가 실행되면서 CA가 계약 내용에 따라 다른 사용자의 EOA로 ETH를 전송하게 된다[9].

합의 프로세스는 현재 비트코인과 같은 PoW를 사용하고 있지만, PoS(Proof of Stake)를 합의 프로세스로 사용하는 이더리움 2.0으로의 하드포크가 진행 중이다. PoS는 소지하고 있는 토큰의 양에 따라 네트워크에 영향력을 행사하는 합의 방식으로 PoW의 과도한 자원 소모를 방지하기 위해 제안된 방안이다. PoS의 보상 구조는 네트워크 유지(블록 생성)에 소요한 자원에 따라 보상을 지급하는 구조이다. 다량의 연산 파워를 가진 소수 노드를 중심으로 EVM(Ethereum Virtual Machine)을 통해 거래 생성 및 실행 처리를 수행한다. 훨씬 적은 수의 검증 노드로 합의를 달성할 수 있으므로 비트코인과 비교하여 합의에 소모되는 지연을 줄이고 트랜잭션 처리량을 향상한다.

하지만 PoW를 수행하는 현재의 이더리움은 초당 트랜잭션 처리 속도 20tps로 스마트계약을 통한 자동화를 통해 비교적 처리량이 증가했지만, 블록체인 위에서 Facebook이나 Amazon과 같이 많은 양의 서비

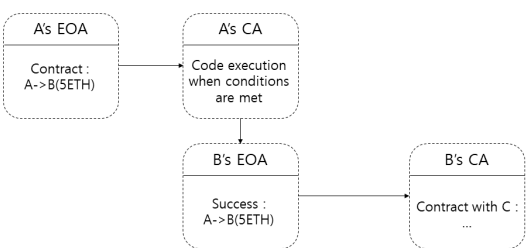

그림 2. EOA와 CA 처리 프로세스
Fig. 2. EOA and CA processing process

스를 제공하는 애플리케이션을 구동하기엔 여전히 부족하다.

PoS 적용을 통해 성능 향상을 기대하고는 있지만, 엉클 블록 생성으로 인한 지연은 여전히 걸림돌이 될 것이다.

엉클 블록은 고아 블록이라고도 부르며, 블록이 같은 시간에 생성되어 블록체인에 fork를 발생[10]시키는 블록을 의미한다.

엉클 블록이 생성되면 [그림 3]와 같이 블록체인은 두 갈래로 나눠진 체인으로 블록 생성이 이뤄지며, 이후 두 갈래 중 길이가 더 긴 체인이 메인 체인이 된다. 이후 나머지 갈래는 블록 자체가 폐기되던 비트코인과 달리 이더리움은 ghost 프로토콜을 통해 해당 블록 정보를 메인 체인으로 수용한다. 하지만, 블록 생성 주기가 15초로 fork가 발생할 가능성이 크기 때문에 해당 수용 과정은 트랜잭션 처리가 지연되는 원인으로 이어진다[11].

또한, PoS가 채택될 경우 네트워크 유지 권한이 소수 노드에 집중됨에 따른 문제점이 존재한다. 경쟁 형태의 블록 채굴을 해야 했기에 시간 순으로 생성된 트랜잭션들을 모두 처리했던 PoW와 달리 PoS는 자신이 소모한 자원에 대해 보상을 받는 방식으로 각기 다른 수수료가 책정된 트랜잭션들에 대해 채굴자는 자신의 이익을 중심으로 처리하게 되며, 상대적으로 보상이 적은 블록은 처리되지 못한 누락 블록이 될 수 있다.

게다가, 중앙만 존재하지 않을 뿐 소수에 의해 좌우되는 네트워크는 블록체인이 추구하는 탈중앙화의 의미가 퇴색되었다고 볼 수밖에 없다.

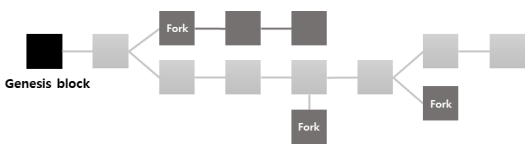

그림 3. 엉클 블록 생성 과정
Fig. 3. Uncle block generation process

2.4 EOS Analysis

EOS는 이더리움을 기반으로 하되 이더리움의 문제점을 지적하며 이에 대한 해결방안을 제시한 가상화폐이다. 또한, 지금까지의 가상화폐들과 달리 사용자에게 수수료가 부여되지 않는 가상화폐이다. 이더리움은 ETH의 소지자가 계약을 실행하면서 코드에 부여된 수수료를 냈었다. 반면, EOS는 [그림 4]와 같이 계약에 대한 주체와 실행자가 나뉘며, 실행자가 거래

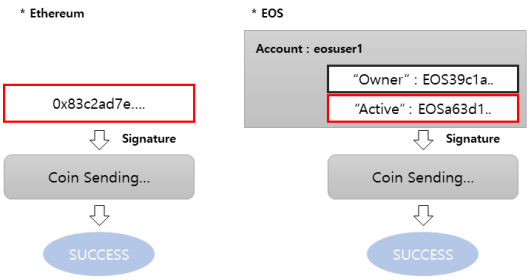

그림 4. 이더리움과 EOS 코드 실행 구조
Fig. 4. Ethereum and EOS code execution structure

에 발생하는 수수료를 대신하여 부담한다. 서비스를 제공하는 DApp들이 사용자 대신에 사용료를 부담하며, 서비스 이용에 특정 암호 화폐 소유를 강제하지 않고 사용자들의 진입장벽을 낮춘다. 하지만, 서비스 제공자에게 부담을 집중시키는 구조는 해당 플랫폼을 통해 서비스를 제공해야 할 이유가 되지 못한다. 때문에, EOS는 DPoS(Distributed PoS)와 스테이킹을 통한 보상 구조로 이 문제점을 해결한다.

PoS가 개인이 소유한 토큰의 양만을 보고 채굴자를 선정했다면, DPoS는 소유한 토큰을 바탕으로 지분 증명 및 지속적인 네트워크 기여도 등의 기준을 통해 네트워크 참여자로부터 선정되어 네트워크 유지에 참여하게 된다.

네트워크 참여자들의 투표를 통해 합의에 참여하는 대표자로 선정된다. 선정된 21명의 대표자로 합의가 진행되며, 과반수의 찬성을 통해 합의되는 PoW와 달리 BFT[12](Byzantine fault tolerance)를 기반으로 2/3 이상의 동의를 얻어야 합의가 이루어진다[13]. 위의 과정을 통해 합의가 진행되며, 블록 생성을 통해 발행되는 암호 화폐 일부를 대표자들에게 지급한다.

DPoS의 보상이 합의에 참여하는 대표자로 제한되었다면, 스테이킹은 누구나 얻을 수 있는 보상이자 네트워크에 참여하는 방법이다.

스테이킹은 자신이 소지한 토큰을 네트워크에 맡기는 행위이다. EOS는 계정이 스테이킹하고 있는 토큰 수에 따라 상태 저장에 사용 가능한 용량이 정해진다[14]. 상태 저장에 필요 용량이 부족할 경우 다른 사용자의 여유분을 대여의 형태로 구매하여 사용할 수 있으며, 스테이킹 참여자들은 네트워크 활동에 참여하지 않더라도 대여를 통한 수익 창출이 가능하다. 서비스 제공자는 개별적인 서비스 제공을 위해 다수의 토큰 스테이킹이 선행되며 규모가 큰 경우에는 대표자로 합의 참여를 통한 수익을 노릴 수 있으며, 그렇지 않더라도 여유분의 스토리지를 대여하여 서비스 제공에

소모된 비용의 일정 부분을 회수할 수 있다. 스테이킹은 소지한 토큰을 보호하는 보안 역할 또한 수행한다. 스테이킹 된 코인은 락업 된 상태라 하며, 해당 상태의 코인은 거래에 사용할 수 없다. 다시 거래에 사용하기 위해서는 언-스테이킹을 통해 원래의 상태로 되돌리기까지 72시간의 대기 시간이 존재한다. 만약 개인키 유출로 인해 공격자가 지갑에 접근하더라도 코인이 락업 된 경우 언-스테이킹을 수행해야 하며, 소지자는 스테이킹/언-스테이킹 여부를 확인할 수 있어 언-스테이킹 되기 이전에 상태 변경 여부를 확인하고 대처할 수 있다.

EOS는 스테이킹을 통해 보상 구조와 보안성 양쪽을 충족하고 있으며, DPoS라는 합의 프로세스로 2000~3000tps에 달하는 트랜잭션 처리 속도 성능을 구현해냈지만, PoS의 문제점을 해결하고자 했음에도 불구하고 결과적으로는 보다 중앙화 된 블록체인이 되었다. 블록체인이 이중지출을 수행하는 51% 공격 등 과반수를 통한 공격이 실제로 실행되기 어려운 이유는 51%가 의미하는 것이 합의에 참여하는 참여자의 수가 아닌 소지한 자원의 양으로 공격에 투자되는 비용에 비해 얻을 수 있는 보상은 적기 때문이다. 그러나 EOS는 대표자가 21명인 반면, 개인에게 주어지는 투표권은 최대 30개로 자신이 희망하는 대표자 및 후보자에 대한 중복 투표가 가능하다. 실제로 현재 대다수의 대표권은 중국계 기업이 쥐고 있으며, EOS 코인이 중국 코인이라 불릴 정도로 장악되어 있다. 대표자 수를 늘리거나 투표권 수를 제한하는 등 특정 집단이 네트워크를 장악하는 비율을 일부 통제할 수는 있겠지만, 탈중앙화 블록체인이라 보기 힘든 것이 사실이다.

2.5 IOTA Analysis

IOTA는 IoT 환경에서의 사용을 목표로 하는 가상화폐로 블록과 체인이 존재하지 않는다. 그럼에도 블록체인의 카테고리에 포함되는 이유는 블록체인의 특성인 DAG(Directed Acyclic Graph)를 기반으로 한 Tangle이라는 구조를 가지기 때문이다.

Tangle은 하나의 노드가 두 개의 노드와 이어진 구조로 노드는 트랜잭션을 의미하며, 하나의 트랜잭션이 새로 생성되기 위해서는 이미 생성된 트랜잭션 중 두 개에 대한 검증이 선행되어야 하는 구조이다[15].

검증을 필요로 하는 노드를 tip이라 부르며, MCMC(Markov Chain Monte Carlo) 알고리즘을 통해 tip을 선별하여 검증을 수행한다. 보조 컨센서스 알고리즘으로 코디네이터가 존재하며, IOTA가 직접 검증에 참여하여 마일스톤을 발행해 MCMC의 작동을 돕는 합의 프로세스를 가진다. 이렇게 트랜잭션을 생성하고자 하는 본인이 직접 검증에 참여하며, 트랜잭션 검증(-)에 대한 대가로 트랜잭션을 생성(+)하기 때문에 거래에 대한 실질적인 수수료가 존재하지 않는다.

IOTA는 블록과 체인이 없으므로 공유 장부를 구성할 수 없으며, 이를 대체하기 위해 IOTA는 스냅샷을 이용한다. 스냅샷을 통해 일정한 주기로 네트워크의 상태를 기록하며, 거래 전체를 캡처하되 소모된 거래를 지우고 남아있는 거래만 tangle의 시작점으로 사용한다. 때문에, 저장하여 관리해야 할 요소는 기존의 공유 장부보다 최소화되어 다른 블록체인들과 비교하여 상대적으로 가벼운 네트워크 운영이 가능하다.

이와 같이 IOTA는 IoT 환경에서의 활용이 적합하도록 네트워크 부담을 최소화하고 tangle 구조를 통해 사용자 증가에 따른 확장성을 가지고 있다. 하지만, 현재 합의 알고리즘에 이용되는 코디네이터가 네트워크에 관여하는 역할이 크다는 점에서 여전히 탈중앙화를 이루지 못하고 있으며, 사물인터넷의 특성에 맞춰 비동기 네트워크인 IOTA는 공격받기 쉬운 형태이다. 또한, 검증이 사용자에게 일임된 구조이지만 모든 사용자가 24/7 작업 검증을 수행하는 것은 실질적으로 불가능하기 때문에 목표치로 설정된 보안이 실제로 제공될 수 있을지는 의문이다.

Ⅲ. 제안하는 아키텍처

비트코인부터 IOTA까지 블록체인의 발전 방향과 각 가상화폐의 특징을 분석해본 결과 트랜잭션 생성부터 검증까지의 flow 및 블록체인 네트워크 간소화를 통한 tps 상승, 수수료 감소를 통한 접근성 향상이 현 블록체인의 발전 방향이며 위 목표를 충족하는 동시에 블록체인의 의의인 탈중앙화를 유지하는 것이 현존하는 블록체인의 공통된 문제점이자 필요 사항이다.

이더리움은 스마트계약을 통한 트랜잭션, EOS는 합의 알고리즘 및 보상 구조, IOTA는 저장구조 자체에 변화를 주는 것으로 기존의 블록체인 대비 성능 향상을 이루어 냈다. 때문에, 본 연구는 블록체인 구성요소 중 성능 향상에 적합한 요소를 찾는 것에서 시작한다.

지금까지의 블록체인의 진화과정을 보면 개선을 위해 지목된 대상이 블록체인의 무결성, 투명성과 같은 고유의 장점을 해치지 않기 위해 거래 방식, 합의 알고리즘 등 대부분 현 구조를 바탕으로 제공하는 서비스 방식에 변화를 주는 방식을 취했다. 하지만 현재까

지의 개선 방향으로는 목표로 하는 성능과 탈중앙화를 동시에 만족시키기엔 한계가 있다. 때문에 본 논문에서는 블록체인에서 무결성, 투명성이 제공될 수 있는 근본인 Distributed Ledger를 중심으로 한 새로운 구조를 제안한다.

Distributed Ledger는 분산 장부 또는 공유 장부라고도 불리며, 블록체인의 거대한 장부로 네트워크 참여자들이 공통의 장부를 소지함을 통해 체인 내에 등록된 트랜잭션들에 대한 무결성을 증명하는 중심 요소이다. 하지만, 개개인이 거대 장부의 데이터를 소지하고 있어야 하므로 높은 저장용량 및 용량의 지속적인 증가가 요구되며, 블록 추가에 따른 장부 업데이트에 적잖은 시간 및 자원이 소비되기 때문에 블록체인의 확장성과 사용성을 제한하는 원인이 된다[16]. 게다가 새로운 수백, 수천 개의 트랜잭션을 처리해 블록으로 가공하여 무결한 장부 유지를 이루는 해당 프로세스는 발생하는 트랜잭션의 시차를 이용해 악의적인 노드의 의도에 의해 생성되어 무결성을 해치는 'fork'의 원인이 되기도 한다. 위의 문제들을 해결하고자 본 논문에서는 거대한 장부를 공유하는 구조가 아닌 단어 그대로 '분산된' 장부 형태를 제안한다.

설명하기에 앞서 제안하는 구조에서 생성되는 트랜잭션 ID는 ① 작성에 사용된 UXTO(Unspent Transaction Output) + ② 새로운 UXTO를 소지하게 될 수신자의 최근 거래를 해시한 값으로 지정한다. ①은 과거 거래 내역 추적을 위해, ②는 트랜잭션 생성 시간 추적을 위한 값으로 이후 제안하는 프로세스에서 활용된다.

3.1 Distributed Ledger

제안하는 구조는 개개인이 해시 트리 구조의 개인 장부를 소지하는 것에서 시작한다. 해시 트리 중 베이스로 사용하는 것은 머클 트리로 [그림 5]와 같이 이진 노드 구조를 가진다. 부모 노드는 두 자식 노드의 값을 해시 한 값을 가지며, 최종적으로 루트는 트리를 구성하는 모든 노드를 해시 한 값을 가진다. 때문에, 구성 노드 중 하나의 값이 변경될 경우 해당 노드의 부모 노드들을 포함하여 루트 값이 변경되는 구조로 위변조 감지가 쉬운 구조이다.

하지만 해시 값으로 분류되는 머클 트리는 특정 트랜잭션을 찾는 탐색 기준이 없으며, 상태 전이에 따라 재계산에 소모되는 시간이 크다. 따라서 머클트리를 기반으로 한 패트리샤 트리[17]를 제안한다. 패트리샤 트리는 머클트리와 기수트리의 특성이 합쳐진 트리로 각 트랜잭션의 상태를 Key-Value를 통해 쉽게 찾을

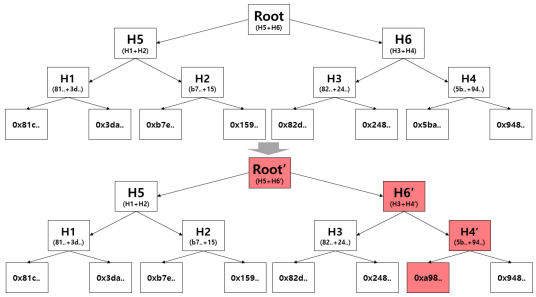

그림 5. Merkle Tree 구조 및 상태변화
Fig. 5. Merkle Tree structure and state change

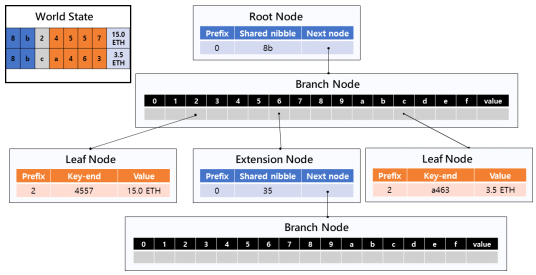

그림 6. Patricia Tree 구조
Fig. 6. Patricia Tree Structure

수 있다.

이 특징을 이용해 자신과 연관된 트랜잭션만을 관리하여 프라이버시를 유지하면서도 개인이 소지한 데이터의 위변조 가능성을 차단하는 개인 장부를 제안한다.

제안하는 장부 구조도는 [그림 7]과 같으며 소비되지 않은 트랜잭션 UXTO와 소비된 트랜잭션으로 분류된 두 묶음으로 나뉜다. UXTO는 트랜잭션이 가진 value의 단위에 따라 구분하여 거래조건에 맞는 UXTO 탐색을 단순화하며, 사용된 트랜잭션은 영수증 항목으로 Key-Value가 변경되어 관리된다. 영수증은 크게 월별 및 Year 노드를 합한 13개의 노드로 구성되며, 년 단위로 12월분의 장부를 해시하여 불필요한 데이터가 과도하게 쌓이는 것을 방지한다. 사용 여

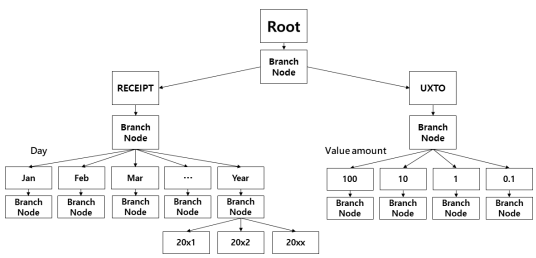

그림 7. 제안하는 Patricia Tree 기반 장부
Fig. 7. Proposed Patricia Tree-based ledger

부, 시간의 변화에 따라 장부 내에서 Key-Value 변경 및 Branch Node 별 해시 값 변동은 발생하지만, 루트 값은 추가되는 트랜잭션에 따른 변동만 있을 뿐 장부 내 변화에 영향을 받지 않기 때문에 상태 전이에 따른 잦은 연산은 이루어지지 않는다.

제안하는 개인 장부는 해시 트리 구조로 무결성을 유지하면서도 상태 변이에 따른 연산을 최소화하여 장부의 활용도를 높이고 있다. 다만, 기존의 블록체인과 달리 공개되는 정보가 한정된 제안하는 구조는 상태 변이에 따른 장부 업데이트가 올바르게 이뤄지는지 검증할 수단이 없다. 이를 보완하기 위해 이웃 노드들로 구성된 peer 네트워크를 형성한다.

일반적으로 블록체인에 참여하는 노드들은 네트워크를 형성하여 자신이 발생한 트랜잭션을 주변 노드에게 전달하고, 그렇게 전달받은 정보를 또 다른 주변 노드에 전파하는 방식으로 네트워크 전체에 정보를 전달하고 공유 장부를 형성한다. 때문에, 특정 트랜잭션 검증 등 필요시 장부 정보 제공을 위해 전체 장부를 갖는 일부 노드를 제외하고도 대부분의 노드들은 필요 이상의 장부 내역을 소지하게 된다. 반면, 제안하는 개인 장부는 위와 같이 정보 공유를 위한 네트워크는 필요하지 않으며, 부족한 신뢰성을 보충하기 위한 목적으로 일부 이웃 노드로만 구성된 peer 네트워크를 가진다.

8개로 구성되는 이웃 노드는 빠른 상태 공유를 위해 물리적 위치를 기준으로 선발되며 신규 peer 네트워크 형성 활성화 및 악의적인 집단 형성을 방지하기 위해 구성 노드 중 무작위로 선발된 5개의 노드는 주기적으로 교체된다. 고정 되는 3개의 노드는 주기적으로 교체되는 노드에게 지금까지의 상태변화 정보를 공유하는 동시 변조된 정보 공유가 이뤄지는지 서로를 감시한다. 이렇게 형성된 peer 네트워크는 새로운 트랜잭션 발생에 따른 상태변화를 공유하며 이웃 노드의 장부 위변조를 감시한다. 일반적인 스마트 컨트랙트 기반 블록체인은 하나의 거래에 대하여 작성된 코드 배포를 위한 트랜잭션, 코드가 실행되어 작성된 트랜잭션 두 개가 생성된다[18]. 반면, 제안하는 구조는 코드 배포를 위한 트랜잭션만이 블록에 포함된다. 이웃 노드는 트랜잭션 생성에 사용된 코드 다이제스트와 체인에 반영된 값과 대조하여 코드의 존재 및 유효함에 대한 검증을 수행하고 상태 변이를 반영한다. 위의 과정을 통해 이웃 노드는 체인에 기록된 정보에 근거하여 상태 변이에 대한 참/거짓을 판단한다.

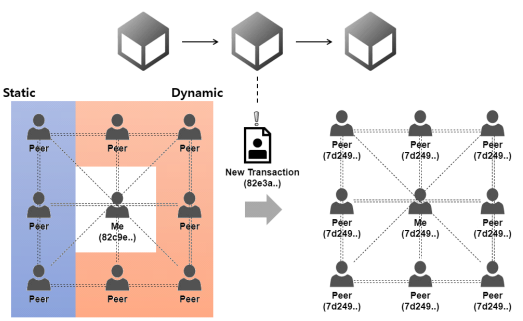

그림 8. Peer Network 및 상태변화도
Fig. 8. Peer network and state change diagram

기존의 블록체인은 신속한 문제해결을 위해 선발된 대표자들을 중심으로 과반수의 동의를 통한 합의가 진행되었으며, 이는 분산장부를 통해 검증에 필요한 정보가 모두 공개되었기 때문에 가능했다. 반면, 제안하는 개인 장부는 체인에 반영되는 정보를 최소화한 만큼 검증을 위한 정보가 제한된 구조이다. 이를 peer 네트워크를 통해 거래 당사자 외의 제삼자를 주기적인 검증자로 내세워 제공되는 정보에 대한 신뢰성을 높인다.

제안하는 구조에서 블록체인에 반영되는 트랜잭션은 코드 배포에 필요한 트랜잭션에 한하며, 이후 거래 당사자 간의 트랜잭션은 개인 장부에 기록된다. 때문에, 코드를 실행하여 트랜잭션을 생성하고 이를 블록으로 생성하여 반영하기까지의 프로세스가 생략되어 있다. 블록체인을 거래에 사용되는 스마트코드의 배포 및 검증의 용도로만 활용하고 이후 프로세스는 거래 당사자 사이에서 진행하여 블록체인 네트워크에 기록되는 정보 및 프로세스를 최소화하는 것이 해당 구조의 목적이다.

3.2 Consensus Algorithm

합의 알고리즘은 블록체인에서 검증자 선발 및 생성된 블록을 체인에 반영하는 방식 모두를 포함하는 말로 가장 중요한 프로세스인 동시 항상 문제점으로 꼽히게 되는 요소이다. PoW는 자원의 낭비 및 투기 조장, PoS와 DPoS는 많은 자산을 보유할수록 보상을 받을 확률이 높은 지분 증명의 특성으로 인한 빈부격차의 심화, Tangle은 개인 검증 방식의 취약점 및 특정 노드에 권한이 집중되어있는 중앙화 등 각각의 블록체인이 채택한 합의 알고리즘들은 각기 다른 문제점을 가지고 있다. 이러한 기존 합의 알고리즘 문제를 해결하면서도 제안하는 구조에 맞는 PoB(Proof of Believability)기반 합의 프로세스를 제안한다. PoB는 개인의 자원 보유량을 기준으로 진행된 기존의 지분 증명에 노드의 신뢰지수라는 새로운 항목을 추가한

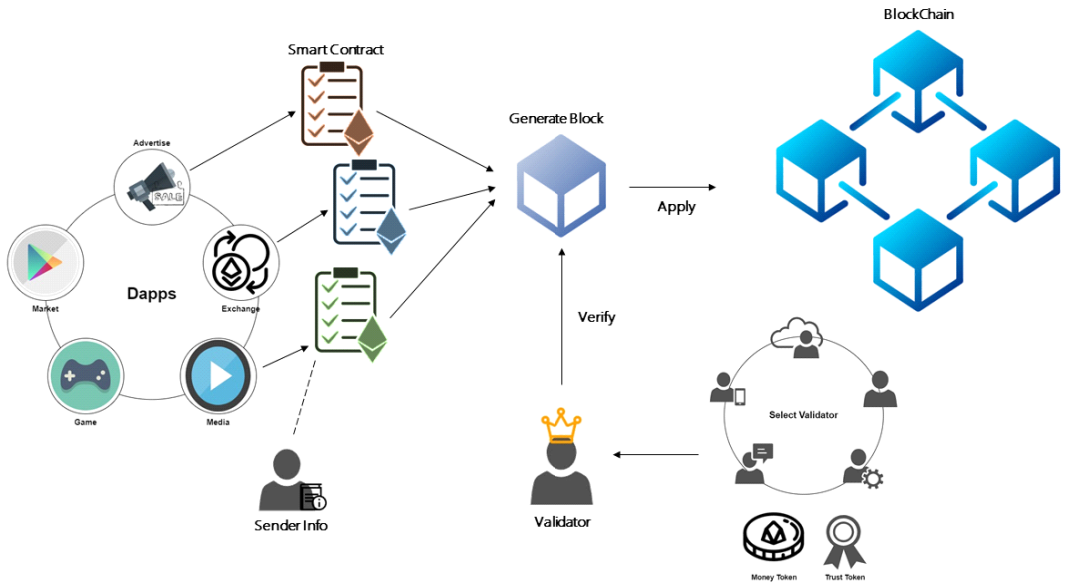

그림 9. 제안하는 PoB 기반 합의 알고리즘
Fig. 9. Proposed PoB-based consensus algorithm

알고리즘으로 후보 노드군 중에 노드의 신뢰지수가 가장 높은 노드에게 거래를 검증할 수 있는 권한과 혜택을 부여하는 알고리즘이다.

검증 노드로의 선발은 먼저 해당 검증을 위한 충분한 연산력을 보유하고 있는지를 확인하기 위해 지분 확인을 통한 후보군 선정이 이뤄진다. 이후 해당 네트워크 생태계 내에서 노드가 해온 활동 및 거래들을 기반으로 한 신뢰도를 나타내는 별개의 토큰으로 정해지며, 검증 노드는 해당 토큰을 다수 보유한 노드 중 무작위로 선별된다. 이전 및 매매를 할 수 없다는 특성을 가진 해당 토큰은 지속적인 활동을 통해서만 쌓을 수 있기에 신뢰를 측정하는 기준 값이 되며, 검증 노드로서 역할 수행이 끝나고 나면 해당 토큰은 파괴되어 0이 된다. 다시 검증 노드로 참여하기 위해서는 일정 수준 이상 신뢰 토큰을 쌓을 필요가 있으므로 아무리 많은 자원을 보유하고 있더라도 체인 검증을 독점할 수 없는 구조이다.

제안하는 PoB 기반 합의 프로세스는 스마트계약을 바탕으로 한다. 검증 노드를 포함한 서비스 제공자들은 PoS와 동일하게 스테이킹 한 자원을 기반으로 네트워크에 영향력을 행사할 수 있으며, 락업 상태로 인한 자원 동결을 기본으로 한다. 앞서 제안된 구조에 따라 트랜잭션 생성 및 검증은 개인이 소지한 장부를 기반으로 수행되며, 블록체인에서 참조할 수 있는 정보는 스마트계약을 배포하기 위해 선행 생성된 트랜잭션에 한정한다. 서비스 제공자에 의해 작성된 코드는 배포를 위해 체인에 등록되며, 배포된 코드를 바탕으로 거래 실행 및 생성된 트랜잭션 검증이 진행된다. 검증과정에서는 체인 내에 기록된 코드와 실제 거래에 사용된 코드 대조, 송신자 정보, 거래에 사용된 UXTO의 무결성 검사가 이뤄진다. 코드가 실행되면 [그림 4]의 EOS와 동일하게 거래 당사자 외의 참여자인 “Active”가 코드 실행 및 검증을 대신 수행하며, 사용자는 사용료(수수료)를 내지 않는다. 사용자에게 수수료를 부과하지 않음으로써 서비스 이용에 대한 진입장벽을 낮추고, 서비스 제공자는 참여 네트워크 내 노드로써 지속적인 기여를 대가로 쌓아온 신뢰 토큰을 사용하여 블록 생성 및 보상을 획득하는 선-순환 구조를 형성한다.

검증과정에서 문제가 발생하였을 경우 기존 검증 노드 외 추가 검증 노드 2개를 선발한다. 노드 선발은 기존 검증 노드 선발과 같은 방식으로 진행하되 분쟁 해결 상황에 한하여 신뢰 토큰은 파괴되지 않는다. 추가된 검증 노드는 거래에 사용된 스마트코드, peer 네트워크가 유지하고 있는 상태 변이 정보와 거래에 사용된 장부 충돌 여부 등에 대한 검증을 수행한다.

선발된 검증 노드 + peer 네트워크 참여자로 구성된 11명간의 합의가 진행되며 결과에 따라 분쟁 발생 노드는 소지한 신뢰 토큰이 파괴되고 보상에 대한 책임을 지닌다. 추가 선발된 검증 노드는 신뢰 토큰,

peer 네트워크 참여자들은 화폐 토큰 보상을 받는다. 네트워크의 권력을 중심 검증 노드에 집중하지 않고 일반 노드에 이를 분산하여 적극적인 네트워크 참여를 유도하는 것이 해당 분쟁 해결 방식의 목적이다.

제안하는 합의 프로세스는 마이닝파워를 바탕으로 한 기존의 공격 가능성을 차단한다. PoB는 무작위로 검증 노드 선별이 이뤄지는 특성상 선별 자격을 충족시켜도 의도하는 타이밍에 선별되는 것은 어렵다. 선별되더라도 블록체인에 등록된 스마트코드를 실행하는 거래 프로세스상 위변조를 위해서는 위조 코드 등록이 선행되어야 한다. 그러나 수정할 수 없는 체인에 등록된 코드는 앞서 설명한 분쟁 해결 과정에서 위변조를 확인할 수 있는 증거가 된다.

신뢰 토큰의 비중이 큰 해당 알고리즘은 지분 증명 알고리즘에 대비하여 필요한 공격 비용이 상대적으로 적다. 그러나 그만큼 신뢰 토큰을 쌓기 위한 장기적인 시간 투자가 필요하며, 공격을 시도하더라도 행위에 대한 증거가 남는 프로세스로 인해 공격이 실행되어도 의미가 없어진다.

3.3 Double Spending Protection

지금까지 제안한 블록체인 구조는 패트리샤 트리 구조를 활용해 개인이 가지고 있는 장부 내용에 대한 무결성을 증명한다. 또한, 자원 외에 신뢰 토큰이라는 요소를 바탕으로 검증 노드를 선발하며 스테이킹을 통한 자원 동결 및 분쟁 해결 시나리오로 블록 생성 및 검증 자격을 이용한 위변조 가능성을 차단하고 있다. 하지만 제안된 구조에 따르면 검증대상은 트랜잭션 실행을 위해 작성된 스마트코드 및 송신자 장부의 무결함에 한정되며, 서로 다른 트랜잭션에 대한 두 코드 모두 송신자의 상태 정보와 일치한다면 이중 지불이 발생하더라도 이를 올바른 거래로 처리하게 된다.

기존의 블록체인에서는 UXTO의 소비성과 잠금 스크립트와 해제 스크립트를 통해 거래의 무결함을 증명했다. 공개키 해시 값과 명령어들로 구성된 잠금 스크립트 'ScriptPubkey', 서명 해시 값과 명령어들로 구성된 해제 스크립트 'ScriptSig'는 자신이 소유한 UXTO에 대한 증명에 필요한 값들이다.

잠금 스크립트가 자물쇠라면 해제 스크립트는 열쇠로, 두 스크립트는 트랜잭션이 발생하면 사용될 UXTO의 소유권 증명 과정에서 스택 구조로 활용된다. 먼저, 해제 스크립트 내의 명령어에 따라 UXTO에 사용된 서명 값과 공개키 값이 스택 내에 순서대로 PUSH 된다. 이후 잠금 스크립트의 명령어 들이 순서대로 PUSH 된다. 먼저 OP_DUP, 복사 명령어에 따라 스택 상단의 공개키가 복사된다. 이후 OP_HASH160에 따라 공개키 해시가 만들어지며, OP_EQUALVERIFY를 통해 잠금 스크립트 내에 있던 공개키 해시 값과 비교하는 과정이 진행된다. 공개키 값은 타원곡선 전자서명 알고리즘 ECDSA에 따라 개인키를 활용해 만들어지는 값으로, 여기까지의 과정은 개인키 소지 유무를 확인하는 소유권 증명 과정에 해당한다. 마지막으로 스택 내에 남아있는 서명을 앞에서 복사 후에 남은 공개키로 해싱하여 트랜잭션에 기록된 값과 호환 여부를 확인한다[19]. 위와 같은 과정을 통해 한번 소유권이 양도된 UXTO는 다른 거래에 사용될 수 없으며, 거래에 대한 무결성을 증명하고 이중 지불을 방지할 수 있다. 이와 같이, 블록체인에서 한번 소비된 UXTO에 대한 중복 거래는 고아 블록으로 분류되어 거래가 인정되지 않았다.

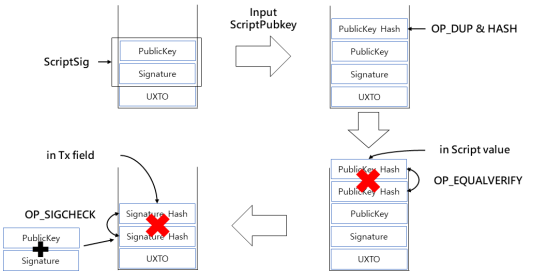

그림 10. 잠금 스크립트 및 해제 스크립트 활용
Fig. 10. Leverage lock and unlock scripts

반면, 장부가 공유되는 기존의 블록체인과 달리 정보 공유가 제한된 현 구조에서 이전과 같이 선행 처리된 트랜잭션 내역을 통한 검증은 불가하다. 거래를 위해 제공된 UXTO에 대해 이미 거래에 사용된 트랜잭션인지 확인할 수단이 없기에 이중 지불이 발생하더라도 이를 정상적으로 수행하게 된다. 이를 방지하기 위해 앞서 제안한 방안에 따라 새로운 검증 구조를 제안한다.

생성되는 트랜잭션 ID에 포함되는 두 값 송신자의 UXTO와 수신자의 최근 트랜잭션은 해당 트랜잭션 생성에 관여한 두 노드의 장부에 보관되어있는 값으로 거래 당사자 외에는 알 수 없는 값이다. 제안하는 검증 구조에는 트랜잭션 ID 생성 규칙을 활용하기 위한 새로운 명령어를 스크립트에 포함하며 [그림 11]과 같다. UXTO를 사용하려는 노드는 해당 UXTO ID를 생성에 사용된 값 중 최근 트랜잭션에 대한 값을 가지고 있다. 해당 값을 'PUSH'하는 명령어를 추가하는 것으로 시작한다. 명령어가 실행되면 개인 장부에서 사용하려는 UXTO의 생성 일자를 기준으로 가장 최

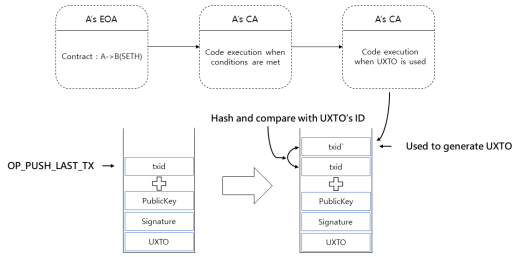

그림 11. 개선된 검증 구조
Fig. 11. Improved verification structure

근에 발생한 트랜잭션 ID 값을 PUSH 한다. 스택에 삽입된 값을 활용하기 위해서는 하나의 CA가 사용되는데, 해당 CA는 거래에 사용되는 UXTO를 생성하는 과정에서 생성된 CA이다. 해당 CA는 UXTO가 생성될 당시 송신자가 생성한 계약 계정으로 UXTO가 거래에 사용된다는 조건하에 실행되며, 송신자가 UXTO 생성에 사용한 이전 UXTO의 ID 값을 제공한다. 이 값을 PUSH 된 값과 함께 해싱하여 생성된 값이 사용하려는 트랜잭션 ID 값과 같다면 올바른 사용자를 통해 사용되는 거래로 판단되며, 이후 잠금 스크립트와 해제 스크립트를 통한 소유 및 유효 검증이 진행된다.

제안하는 검증 구조의 핵심은 공유키의 특성을 활용하는 것이다. 지금까지의 블록체인에서 생성된 트랜잭션 ID 값은 모두 블록체인에 등록되었다. 반면, 제안하는 블록체인은 코드 배포를 위한 트랜잭션만이 등록되며 두 노드 간의 거래 과정에서 생성된 트랜잭션은 공개되지 않는다. 생성된 트랜잭션 ID 역시 각 노드가 가지고 있는 값을 조합해 만들어지는 값으로 공유되는 대상은 거래에 참여한 두 노드와 각 노드의 peer 네트워크 참여자들로 한정된다. 지금까지의 블록체인은 특정 트랜잭션의 개인키가 유출된다면 코인이 도용[20]될 수 있으며, 실제로 키 유출 보안사고가 여러 번 발생했다. 반면, 증명 이전에 진행되는 트랜잭션 ID 조합 과정에 필요한 값은 개인 장부에서 제공되는 값으로 실제로 거래에 참여한 당사자만이 알 수 있는 값이다. 따라서 개인키 유출 사고가 발생하더라도 개인 장부 전체가 유출되지 않는 이상 해당 트랜잭션을 다른 노드가 도용할 수 없게 된다.

조합에 함께 사용되는 값이 CA를 통해 제공되는 이유는 목적으로 하는 이중 지불을 방지하기 위해서이다. 해당 CA는 다른 계정들과 달리 인자 값 전달의 수단으로 사용되지만, 스마트코드 특성상 gas limit를 통해 실행 횟수를 제한할 수 있다. 이점을 이용하여 하나의 UXTO를 사용하는 두 개의 거래 요청이 동시에 발생하였을 때, gas limit에 의해 하나 또는 둘 모두에 대한 거래에 대한 검증이 정상적으로 진행되지 못해 취소되며 이중 지불이 발생하는 상황을 방지할 수 있다.

표 1. 기존 블록체인과 제안하는 블록체인 비교
Table 1. Comparison of general blockchain and proposed blockchain

	General Blockchain	Proposed Blockchain
블록체인 구조	공유 장부와 전체 네트워크	개인 장부와 peer 네트워크: 데이터 관리 및 처리량 감소, 네트워크 규모 감소를 통한 전반적인 간소화
합의 알고리즘	PoW, Pos 등 경쟁 방식의 합의 알고리즘	PoB 기반 합의 알고리즘: 신뢰토큰 중심의 검증 자격 부여 → 경쟁으로 인한 자원 낭비 및 네트워크 과부하 해소
인증 구조	잠금, 해제 스크립트	CA를 활용한 검증: 이중 지불 및 개인키 유출로 인한 도용 가능성 방지

Ⅳ. 결론 및 향후 연구 방향

필자가 제안하는 블록체인은 기존 블록체인에 있던 문제점을 해소하면서도 안전성이 감소한 2, 3세대 블록체인과 달리 보안을 강화하였다.

먼저, 공유 장부에서 개인이 관리하는 장부로 변화하면서 블록체인이 관리 및 처리하는 데이터양이 대폭 감소하였다. 패트리샤 트리 구조를 기반으로 관리되는 개인 장부는 모든 노드의 해시 값이 반영되는 머클트리의 루트의 특성을 통해 중간의 위변조를 쉽게 감지할 수 있다. 또한, peer 네트워크를 형성하여 상태 변이를 추적하고 위변조를 감시한다. 이를 통해 블록체인에 모든 정보를 등록하지 않고도 무결함을 증명할 수 있다.

합의 알고리즘에서는 필요 이상의 자원 소모를 방지하면서도 중앙 집권화가 되는 현 블록체인의 문제 양쪽 모두를 해결하였다. 제안한 PoB 기반 합의 프로세스는 채굴 경쟁을 방지하는 지분 기반 증명에 신뢰 토큰을 추가했다. 네트워크 내 기여도에 따라 지급되는 해당 토큰은 거래가 불가하며 검증 노드 선발에 사용된 이후에는 파괴된다. 때문에, 자원의 보유량에 관계없이 특정 기업 또는 단체가 블록체인을 독점하는 것은 불가능하다. 신뢰 토큰이 검증 노드로 선발되는 데 차지하는 비중이 크기 때문에 네트워크 내에서 기

여도를 쌓는 것이 중요하며 이 점을 이용하여 스마트 코드 작성 및 실행 등 사용자가 서비스를 이용하는데 필요한 비용을 대신 부담하며 토큰을 쌓고 사용자는 해당 블록체인에 별도의 진입비용 없이 서비스를 활용할 수 있다.

제안하는 스크립트 검증에서는 개인 장부를 이용한 검증과정에서 발생할 수 있는 문제점을 해결하면서 보안사고의 발생 여지를 차단한다. 트랜잭션 ID 값 부여 법칙을 활용한 해당 검증 구조는 잠금, 해제 스크립트를 사용하기에 앞서 사용자 인증 과정이 진행되며 UXTO 생성에 관여한 두 사람만이 알 수 있는 값으로 진행되는 검증은 개인키 유출로 인해 UXTO가 도용되는 가능성을 차단하며, 검증과정에서 활용되는 CA는 이중 지불이 실행되는 것을 차단한다.

전송되는 데이터 량이 방대해졌으나 개개인의 정보 보호가 중요시되는 IoT의 특성에 맞게 공유되는 정보 범위를 최소화하면서 블록체인 고유의 보안성을 유지하였으며, 제안한 알고리즘들은 IoT 환경에서 구현하기에보다 적합하다.

향후 연구에서는 5G와 클라우드의 활용을 위해 제안된 MEC(Multi Edge Computing) 기술을 제안한 아키텍처에 대입하여 에지 서버를 활용한 성능 향상을 위한 연구를 진행할 예정이다.

References

[1] I. S. Son, "5G IoT technology trend and prospect," *The IEIE*, vol. 46, no. 4, pp. 56-63, Apr. 2019.

[2] Y. H. Jeon, "A study on the security modeling of internet of things(IoT)," *KIIT*, vol. 15, no. 12, pp. 17-27, Dec. 2017.

[3] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Overcoming limits of blockchain for IoT applications," in *Proc. 12th Int. Conf. availability, Reliability and Secur.*, pp. 1-6, New York, United States, Aug. 2017.

[4] J. Huang, L. Kong, C. Chen, and M. Y. Wu, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3680-3689, Mar. 2019.

[5] National Archives and Records Administration, *Blockchain White Paper*, pp. 1-13, Feb. 2019.

[6] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*(2009), Retrieved May 21, 2020, from https://bitcoin.org/en/bitcoin-paper.

[7] S. R. Kim, "Legal restrictions and limitations of blockchains and bitcoins," *Hannam J. Law&Technol.*, vol. 24, no. 3, pp. 119-120, 2018.

[8] S. M. Habibul, F. Jahan, S. M. Sara, and D. Nandi, "Secured blockchain based decentralised internet: A proposed new internet," *Int. Conf. Computing Advancements*, pp. 1-8, Sapporo, Japan, Jan. 2020.

[9] V. Buterin, *Ethereum Whitepaper*(2013), Retrieved Jun. 3, 2020, from https://ethereum.org/en/whitepaper/.

[10] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," in *Proc. 6th Int. Conf. Principles of Secur. and Trust*, pp. 164-186, Uppsala, Sweden, Apr. 2017.

[11] A. Shurov, D. Malevanniy, O. Lakushkin, and V. Korkhov, "Blockchain network threats: The case of pow and ethereum," *Int. Conf. Computational Sci. and Its Appl.*, pp. 606-617, Saint Petersburg, Russia, Jun. 2019.

[12] M. A-E-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-scalable byzantine fault-tolerant services share on," *ACM SIGOPS Operating Syst. Rev.*, vol. 39, no. 5, Oct. 2005.

[13] D. Larimer, *EOS. IO technical white paper v2*(2018), Retrieved Jun. 10, 2020, from https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[14] Z. Cole, "*EOS: An Architectural, Performance, and Economic Analysis*(2018)," Retrieved Jun. 15, 2020, from https://hackernoon.com/eos-an-architectural-performance-and-economic-analysis-43a466064712?source=rss----3a8144eabfe3---4.

[15] M. Divya and N. B. Biradar, "IOTA-next generation blockchain," *Int. J. Eng. and Comput. Sci.*, vol. 7, no. 4, pp. 23823-23826, Apr. 2018.

[16] J. Y. Lee, "Security and implications of

FinTech based block chain," *Rev. KCA*, vol. 16, no. 2, pp. 25-27, Jun. 2018.

[17] G. Wood, "*Ethereum: A secure decentralised generalised transaction ledger, Byzantium version*(2018)," Retrieved Jul. 18, 2020, from https://ethereum.github.io/yellowpaper/paper.pdf

[18] C. J. Kim, "A static and dynamic design technique of smart contract based on block chain," *Korea Academy Ind. Cooperation Soc.*, vol. 19, no. 6, pp. 110-119, Jun. 2018.

[19] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media, pp. 132-143, 2017.

[20] Financial Security Institute, *Blockchain technology and security considerations*(2017), Retrieved Sep. 11, 2020, from https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/1267.do.

이 승 호 (Seungho Lee)

2019년~현재 : 건국대학교 컴퓨터정보통신공학과 석사과정

<관심분야> 블록체인, 사이버보안, IoT

[ORCID:0000-0002-8142-5136]

김 기 천 (Keecheon Kim)

1992년 : Northwestern Univ. 공학박사

1998년~현재 : 건국대학교 컴퓨터공학과 교수

<관심분야> 통신공학, 미래인터넷, 사이버보안, IoT

[ORCID:0000-0003-3445-3334]