블록체인 플랫폼에서의 합의 알고리즘

이부형, 임연주, 이종혁
상명대학교 프로토콜공학연구실

{boohyung, yeonjoo, jonghyouk}@pel.smuc.ac.kr

Consensus algorithms in blockchain platforms

Boohyung Lee, Yeon-Joo Lim, Jong-Hyouk Lee
Protocol Engineering Lab., Sangmyung University

요 약

사물인터넷 시대가 도래하면서 분산 원장 기술과 서로 신뢰하지 않는 사용자 간의 합의 알고리즘을 이용한 블록체인이 네트워크의 패러다임을 변화시킬 화두로 떠오르고 있다. 본 논문에서는 블록체인의 정의를 설명하고, 현재 서비스 중인 블록체인 플랫폼에서 사용하는 합의 알고리즘의 개념 및 특징을 설명하였다.

Ⅰ. 서 론

4 차 산업혁명이 도래하면서 사물인터넷과 인공지능을 기반으로 전 세계가 네트워크로 연결되는 시점에서 현재보다 약 20 배 이상의 사물들이 인터넷에 연결되어 네트워크를 이룰 전망이다. 그로 인해 중앙집중식으로 수많은 데이터를 주고받는 기존 방식으로의 운영이 어려울 것이라고 예상하고 있다.

본 논문에서는 분산 데이터베이스 형태로 지속적으로 생성되는 데이터 기록 리스트를 임의 조작이 불가능하도록 고안된 블록체인에 대하여 정의한다. 또한, 서로 신뢰하지 않는 네트워크 사용자들간의 신뢰를 확보하고 블록체인 내의 데이터를 항상 최신 버전으로 유지하는 방법으로 사용하는 합의 알고리즘에 대해 설명한다.

본 논문의 2 장에서는 블록체인의 정의와 블록의 구성, 구현 방법에 따른 분류에 대해 기술한다. 3 장에서는 대표적인 퍼블릭 블록체인 플랫폼에서 사용하는 합의 알고리즘의 개념 및 특징을 소개하며, 4 장에서 본 논문을 결론짓는다.

Ⅱ. 블록체인

블록체인은 2008 년 사토시 나카모토가 처음 제안한 비트코인 (Bitcoin) [1] 이라는 디지털 통화 기술에서, 디지털 통화를 안전하게 저장하여 사용자 간에 주고받기 위해 위해 만들어진 기술이다. 비트코인은 애초에 중앙에서 통화를 발행하고 관리하는 기관없이 P2P 네트워크 상에서 오롯이 사용자 간의 안전한 거래가 가능하도록 고안되었다. 블록체인을 구성하는 데이터의 무결성 및 신뢰성을 보장하기 위해 해쉬 함수 (SHA-256)와 디지털 서명 (ECDSA)을 사용한다.

블록체인을 구성하는 블록은 블록 헤더와 블록 바디로 이루어는데, 블록 헤더에는 이전 블록 헤더의 해시값이 들어있어 일종의 체인처럼 링크드리스트 방식으로 모든 블록이 연결되어 있고, 합의 알고리즘에 이용하는 임의의 nonce 값과 블록 생성의 난이도를 조정하는 bits 등이 포함되어 있다. 블록 바디에는 지원하는 서비스에 따라 다른 값이 들어갈 수 있다. 예를 들어, 디지털 암호 통화 시스템인 비트코인에서는 10 분 동안 발생한 사용들 간의 거래가 블록 바디에 포함된다.

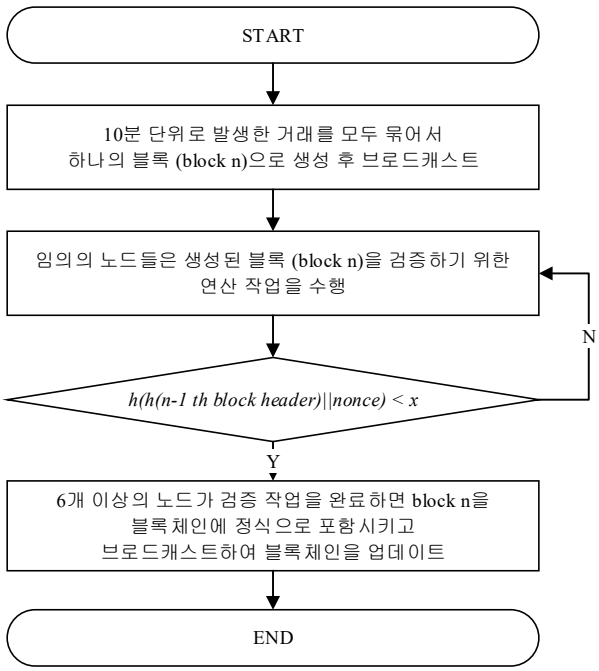
Ⅲ. 합의 알고리즘

블록체인을 사용에 참여하는 사용자라면 누구나 데이터를 입력, 변경 또는 삭제할 수 있기 때문에 제 3 의 신뢰기관 (TTP: Trust Third Party)없이 신뢰성 있는 거래를 하기 위한 근간 기술인 합의 알고리즘의 사용이 반드시 필요하다. 합의 알고리즘을 이용하면 권한이 있는 사용자끼리의 특정 매커니즘 동작 후 블록체인에 저장되는 데이터의 신뢰성을 보장받을 수 있다. 그로 인해 블록체인의 상태가 안전하게 업데이트되고 유지되어, 블록체인 내의 데이터 무결성이 보장된다.

- PoW (Proof of Work, 작업 증명): PoW [2]는 가장 보편적으로 알려진 합의 알고리즘이다. 비트코인에서는 10 분 단위로 발생한 모든 거래를 하나의 블록으로 묶어 시간 순서에 따라 하나의 체인처럼 연결하여 전체 P2P 네트워크 상에 공유한다. 네트워크 내의 노드들은 이전 블록 헤더의 해시값과 nonce 를 연접한 값을 해시 연산하여 특정한 값 x를 찾는 연산을 수행하게 된다. nonce 는 최초 0 부터 시작하여 조건을 만족하는 해시값을 찾을 때까지 1 씩 증가하는 32-bits 의 수이고, x는 몇 개의 0 으로 시작되는 256-bits 의 수이다. 해시 연산의 특성 상 역연산이 어렵기 때문에 x 를 찾기 위해서는 nonce 를 변화시키면서 순차적으로 대입하여 연산하는 과정이 필수적으로 요구된다. 이러한 과정 때문에 컴퓨팅 파워가 높은 노드일 수록 블록 생성에 걸리는 시간은 줄어든다. 해시 연산을 $h(.)$로 표시할 때 (1)과 같은 조건을 만족한다면 n번 째 블록에 대한 증명 작업이 완료된다.

$$h(h(n-1\ th\ block\ \ header)||nonce) < x \quad (1)$$

비트코인에서는 블록 헤더 내의 bits 를 이용하여 x 내 0 의 개수를 1 씩 늘려가며 블록 생성 시간을 10 분으로 일정하게 유지하고 있다. 6 개 이상의 노드들이 연산을 통해 블록 생성에 대한 위와 같은 증명 작업을 완료하면 그 블록을 공식적으로 인정하여 블록체인에 포함시킨다. 위에서 설명한 PoW 동작 과정을 나타내는 순서도는 [그림 1]과 같다.



[그림 1] 비트코인에서의 PoW 동작 과정

- PoS (Proof of Stake, 지분 증명): PoW 의 대안으로 제안되어 개발된 PoS [3]에서는 계산능력이 아닌 화폐의 보유량에 따라 각 노드의 합의 결정권이 달라진다. 만약 노드 A 가 가진 화폐 보유량이 $bal(A)$, t를 타임스탬프, d 를 난이도 조정값이라고 하면 (2)와 같은 조건을 만족할 때 블록 n 에 대한 합의 권한이 노드 A 에게 주어진다.

$$h(h(n-1\ th\ block\ header),t) \leq h(bal(A),d) \quad (2)$$

일반적으로 블록체인을 공격하기 위해서는 공격자가 네트워크의 51% 이상을 점령해야 하는데 PoS 를 사용하면 총 화폐 보유량 중 51% 이상을 가지고 있어야 공격이 가능하므로, PoW 를 사용할 때보다 해커 입장에서 공격에 드는 비용이 매우 증가하여 보안성이 같이 높아진다는 장점을 가진다. 이러한 특징 때문에 최근 이더리움 [4]에서는 합의 알고리즘을 PoW 에서 PoS 로 바꾸려는 움직임이 나타나고 있다.

- DPoS (Delegated Proof of Stake, 위임된 지분 증명): PoS 가 일정한 지분을 가진 모든 노드에게 블록 생성 권한을 주었던 반면, 비트쉐어 [5]에서 사용하는 DPoS [6] 에서는 네트워크를 구성하는 모든 노드들의 투표 결과에서의 상위 101 개의 노드에게만 권한을 부여하여 합의에 대한 권리를 위임한다. 투표에 의해 선출된 대표자들의 신뢰를 바탕으로 블록을 생성하기 때문에 합의에 걸리는 시간과 비용이 적게 소요되고, 단위 시간동안 생성되는 블록의 개수도 PoW 와 PoS 에 비해 상대적으로 많다. 만약 어떠한 블록체인 네트워크에서 노드 A 가 대표자가 되기 위해서는 조건 (3)을 만족해야 한다. (3)에서 $n(Voter_A)$ 는 노드 A 를 대표자로 선출한 사용자의 수, $n(Voter_{al})$ 은 투표에 참여한 사용자의 수를 의미한다.

$$n(Voter_A) > \frac{n(Voter_{al})}{2}$$

대표자들은 매 차수마다 임의로 배정되는 순서에 따라 블럭을 만들어 블록체인에 추가할 수 있는 권한을 가진다. 또한, 대표자간의 투표에 의해 악의의 사용자로 선출된 노드는 블록체인 네트워크에서 추방시킬 수 있어 블록체인 네트워크를 유지하는데 도움을 줄 수 있다. 하지만 블록 내의 발신자, 수신자, 잔고 등은 바꿀 수 없다.

Ⅳ. 결론

본 논문은 블록체인에 참여하는 어느 누구나 거래 참여 및 검증이 가능한 블록체인 플랫폼에서 사용하는 합의 알고리즘인 PoW, PoS, DPoS 를 조사하고 설명하였다.

같은 블록체인을 사용하더라도 제공되는 서비스의 분야에 따라 합의에서 중요하게 생각할 가치는 달라질 수 있다. 그렇기 때문에, 서비스에 따라 효율적으로 사용할 수 있는 합의 알고리즘의 선택이 필요하다. 또한, 현재 블록체인 플랫폼에서 사용하는 합의 알고리즘들은 해결되지 않은 보안 이슈를 가지고 있기 때문에, 효율적으로 서비스에 직접 적용 가능한 알고리즘 개발 노력이 필요하다.

ACKNOWLEDGMENT

본 연구는 2014 년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2014R1A1A1006770).

참 고 문 헌

[1] Satoshi Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, 2008.

[2] Antonopoulos, Andreas M, Mastering Bitcoin: unlocking digital crypto-currencies, OReilly Media, 2014.

[3] “Proof of stake versus Proof of work”, Bitfury Group Whitepaper, 2015.

[4] Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper.

[5] Fabian Schuh, Daniel Larimer, “BITSHARES 2.0: FINANCIAL SMART CONTRACT PLATFORM”, 2015.

[6] Daniel Larimer, “Delegated Proof-of-Stake (DPoS)”, Bitshare whitepaper, 2014.