확장성이 고려된 Bitcoin-NG 프로토콜 고찰 및 연구

김수현*, 차정훈*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail: {ryun71380, ckwjdgns, jhpark1}@seoultech.ac.kr

Consideration and Research of Bitcoin-NG Protocol Considering Scalability

Soo Hyeon Kim*,Jeong Hun Cha*, Jong Hyuk Park*
*Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

최근 IT 기술의 발전에 따라 블록체인 기술과 융합하려는 다양한 시도를 보인다. 비트코인(Bitcoin)의 탄생으로 알려지게 된 블록체인은 P2P (Peer-to-Peer) 네트워크에서 데이터의 무결성 조건을 만족할 수 있게 되면서 보안 기술에 대해 많은 연구가 진행 중이다. 데이터의 무결성을 증명하기 위해 합의 알고리즘을 사용하는데, 합의 알고리즘의 처리속도 및 저장 공간 문제 등으로 인해 다른 분야로 확장에 어려움을 겪고 있다. 따라서 블록체인을 구성하는 환경이나 목표에 따라서 적절한 합의 알고리즘을 선택하는 것이 중요하다. 본 논문에서는 확장성 문제를 해결할 수 있는 Bitcoin-NG 합의 알고리즘을 비롯하여 다양한 합의 알고리즘의 원리와 장단점을 소개한다. 블록의 합의에 참여하는 범위, 리더를 선정하는 방법 등의 기준으로 Bitcoin-NG 알고리즘이 확장성 문제에 긍정적인 합의 알고리즘으로서 갖춘 특징을 살펴보고 앞으로 합의 알고리즘의 발전 방향에 대해 고찰한다.

1. 서론

최근 다양한 종류의 네트워크 장치들이 개발되면서 하나의 네트워크에 P2P 연결이 많아지고 있다. 2008년 '사토시 나카모토'에 의해 처음으로 세상에 알려지게 된 블록체인은 분산 데이터베이스 시스템이다[1]. 블록체인 기술은 블록이 체인에 결합하게 되면 블록의 내용을 수정할 수 없다는 점에서 무결성 조건을 만족하게 되어 보안 기술로 인기를 얻었다. 세계 경제 포럼에서는 12대 유망 기술 중 하나로 블록체인을 선정하였으며, 나아가 약 10년 뒤 전 세계 GDP의 10%가 블록체인 기술에 기반을 둘 것으로 예측한다[2].

블록체인은 P2P 네트워크에서 완전한 정보 공유로 인해 특정 노드를 목표로 하는 해킹 시도를 무력화할 수 있으며, 단일 장애 점 (Single Point Failure) 발생에 대비할 수 있다. 하지만 분산 네트워크를 기반으로 하는 블록체인은 네트워크에 참여하는 노드가 증가하게 되었을 때, 검증해야 하는 거래의 수와 합의해야 하는 대상의 수가 증가하게 되어 네트워크 참여자 간의 합의에 도달하는 시간이 증가하게 된다. 시간이 지날수록 길어지는 체인을 저장하는 점과 블록의 크기가 1MB로 제한되어 큰 데이터를 저장하는 데 어려움이 있다는 점에서 기술적 한계를 보인다.

네트워크 참여자 간의 합의 도달 시간이 증가하는 한계를 극복하기 위해서 속도가 빠른 합의 알고리즘을 사용하고 하나의 프로세스가 처리해야 하는 데이터의 크기를 줄여 동일한 알고리즘에서 빠르게 처리할 수 있도록 한다. 다중 블록체인이나 샤딩 (Sharding) 방법, 병렬처리 또는 분할처리 방식을 이용하여 처리해야 하는 데이터의 크기를 줄일 수 있다. 저장 공간으로 인한 블록체인의 기술적 한계를 극복하기 위해서는 다중 블록체인을 이용하거나 외부에 저장 후 가리키는 키를 이용하는 등의 방법이 있다[3].

본 논문은 비트코인 등의 암호 화폐에서 사용 중인 합의 알고리즘 중 PoW, PoS, DPoS 합의 알고리즘의 원리 및 장단점에 관해서 서술하고, 블록체인의 확장성 문제를 해결할 수 있는 Bitcoin-NG의 구조 및 원리에 대해 소개한다. 마지막으로 처리 속도 및 보안성의 측면에서 합의 알고리즘을 분석하여 확장성을 해결하기 위한 조건에 대해 고찰한다.

2. 다양한 종류의 합의 알고리즘

P2P 연결을 기반으로 하는 블록체인은 거래의 신뢰를 보증해주는 제 3자가 없고, 신뢰할 수 없는 노드들로 네트워크가 구성된다. 발생하는 트랜잭션이 올바른 것인지 증명하고 신뢰 있는 데이터임을 증명하기 위해서 합의 알고리즘이 요구된다. 합의 알고리즘을 통해 블록체인 네트워크에서 모든 노드가 동일한 데이터를 공유하게 된다.

다음은 현재 암호 화폐에서 많이 사용되는 합의 알고리즘에 소개 및 장점과 단점에 대한 설명을 한다.

2.1 Proof-of-Work 합의 알고리즘

비트코인에서 사용하고 있는 합의 알고리즘으로 1993년 DDos 공격과 같은 사이버 공격을 막기 위해서 처음으로 정의되었다. 이후 '사토시 나카모토'에 의해 블록의 합의를 이끌어 내는 합의 알고리즘으로 이용된다.

PoW는 생성하고자 하는 블록의 해시값에 맞는 논스 (Nonce) 값을 찾는 방법으로 0부터 1씩 증가시키면서 찾는다. 블록 생성 주기는 해시 난이도를 통해 조절하는데, 평균적으로 소요 시간을 10분으로 설정했다. 주기적으로 해시 난이도 조절을 통해 블록 생성 주기를 제어한다[4].

작업 증명 방식 합의 알고리즘은 더 큰 네트워크를 구성할수록 안정성이 증가하고, 간단한 구조로 누구나 참여 가능하다는 장점이 있다. 하지만 네트워크 자원의 51%를 차지하게 되면 네트워크 전체 합의를 좌우할 수 있다는 점과 불필요한 컴퓨터 자원을 많이 사용한다는 한계점을 보인다.

2.2 Proof-of-Stake 합의 알고리즘

PoW가 에너지 소비에 의존한다는 점을 지적하며 Coin age라는 개념을 도입하여 합의에 이용되는 불필요한 컴퓨터 자원 사용을 줄이고자 했다.

PoS는 통화의 소유권 증명 형식을 의미하며, 새로운 블록을 추가하기 위해서는 자신이 보유한 코인을 자신의 블록에 등록함으로써 다음 블록 생성자로 선택될 확률을 높이는 방법이다[5]. (수식 1)은 PoS의 해시 함수와 채굴 난이도 사이의 관계를 나타낸다[6].

$$hash(hash(B_{prev}),A,t) \leq bal(A)M/D \qquad (1)$$

B_{prev}은 이전 블록의 Target 값, A는 주소 (Address), t는 해당 블록의 타임스탬프, bal(A)은 A가 가진 지분에 비례하는 Balance, D는 암호 퍼즐의 난이도, M은 암호 퍼즐이 가질 수 있는 난이도의 최댓값을 의미한다. 블록 B의 해시값은 A가 소유한 Balance와 난이도의 영향을 받게 된다. A가 소유한 Balance가 클수록 M의 값은 작아지게 됨으로 많은 지분을 가진 노드가 낮은 난이도의 문제를 풀 게 되어 채굴의 확률을 높여준다[7].

모든 노드가 채굴에 참여하지 않음으로써 생성 주기를 단축할 수 있으며, PoW에서 문제가 되었던 컴퓨팅 낭비를 줄일 수 있다. 하지만 초기 지분이 많은 사람이 다음 블록 생성에 더 유리하다는 단점이 있다. 이를 해결하기 위해 코인의 양 및 코인 소유일수 기반으로 생성되는 수치를 통해 초기 지분이 많은 사람들이 블록 형성을 독점하는 것을 막는 Coin age 개념을 도입했다. 그러나 PoS는 Nothing at Stake가 발생하여 하나의 블록체인을 형성하는 것에 문제를 겪을 수 있다.

2.3 Delegated Proof of Stake 합의 알고리즘

DPoS 합의 알고리즘은 위임 지분 증명 알고리즘을 의미하며, 암호 화폐 소유자들이 각자의 지분율에 따라 투표를 하여 각 네트워크의 대표자를 선정하고 대표자들끼리 합의하여 의사결정을 내리는 방법이다. 대표자가 되고 싶은 노드의 경우 자신을 공개키와 함께 등록하면 네트워크를 구성하는 노드들의 투표를 통해 대표자로 선출될 수 있다.

합의는 네트워크를 대표하는 대표자에 의해서 이루어지기 때문에 합의에 걸리는 시간 및 비용이 적게 사용되고, 단위 시간 동안 생성되는 블록의 개수 또한 많아진다. 실제로 이더리움은 545,224Tx (Total Transactions) 처리속도를, DPoS 합의 알고리즘을 이용하는 스팀 (Steam)은 1,169,182Tx 처리속도를 가진다[8]. 하지만 블록 생성을 대표하는 대표자들 사이에 블록 생성 권한을 계속 유지하기 위해서 서로가 서로에게 투표하는 상황이 발생 할 수 있다. 일반 노드들이 대표자 선출에 있어 적극적으로 투표를 하지 않은 경우, 대표자들 소수의 담합으로 인해 소수 노드에 의해 블록체인의 전부가 지배될 수 있다.

3. 확장성이 고려된 합의 알고리즘 Bitcoin-NG

Bitcoin-NG (Next Generation)는 확장성을 고려

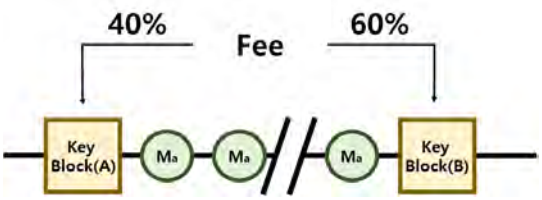
한 새로운 블록체인 알고리즘으로 블록체인 연산을 작업 증명을 이용한 '리더 선택'과 '트랜잭션 직렬화' 두 부분으로 구분한다. 비트코인의 경우 트랜잭션의 처리 시간과 보안성이 반비례 관계를 가졌지만, Bitcoin-NG에서는 보안성을 감소시키지 않고 트랜잭션의 처리 시간을 향상한다.

3.1 Bitcoin-NG 프로토콜의 구조

Bitcoin-NG는 리더를 선출하기 위한 Keyblock과 장부의 역할을 하는 Microblock으로 구성된다. Keyblock은 현재 Unix 시간과 이전 블록에 대한 참조, 논스값 등으로 구성되며 Microblock을 검증할 수 있는 Keyblock 리더의 공개키를 포함한다. Microblock의 헤더에는 이전 블록에 대한 참조, 현재 Unix 시간, 최신 Keyblock의 개인키로 서명된 내용 등으로 구성된다. Keyblock 생성에 성공한 노드를 리더 노드라고 하고, 리더 노드는 다음 리더가 선정되기 전까지 Microblock을 생성할 수 있는 권한을 가지게 된다. Keyblock의 개인키로 한 서명을 통해 Microblock의 유효성을 입증하게 된다.

3.2 Bitcoin-NG 프로토콜의 작동 원리

시간을 에폭 (Epoch)으로 나누어, 각 에폭마다 하나의 리더를 가지게 된다. PoW와 동일하게 Key block 헤더의 해시는 Target value보다 작도록 논스값을 변경하며 암호 퍼즐을 푼다. (그림 1)는 Bitcoin-NG의 체인 구조로 노드 A에 의해 생성된 Microblock은 노드 A의 개인키로 서명되어 있으며, 생성되는 Microblock의 수수료는 해당 Keyblock에게 40%, 다음 생성되는 Keyblock에게 60%로 나눈다.



(그림 1) Bitcoin-NG의 체인 구조 [9]

새로운 Keyblock을 생성한 노드가 보다 트랜잭션 처리를 통한 이득을 증가시키기 위해 이전 Keyblock을 생성한 노드가 생성한 Microblock을 일부러 배제하는 것이 가능하다. 이것을 막기 위해 현재 Keyblock이 생성한 Microblock에서의 수수료를 다음 Keyblock과 나눈다.

Bitcoin-NG는 Microblock에서는 PoW 작업을 포함하지 않음으로 쉽고 빠르게 생성될 수 있다는 장점이 있다. 하지만 포크 발생 및 이중 지불 문제 (Double-Spending)가 발생하기 쉽다는 문제점을 가진다.

4. 확장성이 고려된 합의 알고리즘에 대한 고찰

블록의 합의에 참여하는 범위, 리더를 선정하는 방법 등에 따라서 다양한 합의 알고리즘이 존재한다는 것을 확인했다. PoW는 모든 노드가 채굴의 대상이 될 수 있으며 채굴을 통해 더 빠르게 논스 값을 찾아내는 노드가 블록을 생성하여 모든 노드가 합의에 참여하는 방법이다. PoS는 자신이 가진 지분에 의해 암호 퍼즐의 난이도가 반비례로 조정되어, 많은 지분을 가질수록 논스를 찾아내는 것이 쉽다. 지분에 따라 채굴할 노드를 결정하고 채굴을 통해 생성된 블록은 네트워크를 구성하는 모든 노드의 합의를 통해 체인에 연결되게 된다. DPoS는 네트워크에 포함된 모든 노드들이 지분 등록을 통해 대표자를 선정함으로써 블록의 합의에 참여하는 노드를 대표자 집합으로 제한한다. 대표자들에 의해 합의 과정에 진행되기 때문에 블록을 생성하여 체인에 연결하는 속도는 빠르지만, 탈중앙화로부터 멀어지게 된다. Bitcoin-NG는 PoW의 방법을 이용하여 네트워크에 포함된 모든 노드들이 리더 선출에 참여한다. 특정 노드가 리더로 선정된 후 공개키 기반 암호 기술을 이용하여 여러 개의 Microblock을 생성하게 되고, 네트워크에 포함된 모든 노드들이 공개키로 확인함으로서 합의를 이루게 된다. 공개키 암호를 이용하여 시간이 오래 걸리고 자원을 많이 사용하는 채굴을 한 번만 실행하고 여러 개의 블록을 체인에 연결하는 방법을 통해 트랜잭션의 처리속도를 증가시켰다.

모든 노드가 블록을 생성하는 과정과, 합의를 이끌어 내는 과정에 참여하여 많은 검증을 거치는 방법이 보안성에 이득을 보인다. 하지만 모든 노드가 참여함으로써 거쳐야 할 과정이 늘어나 처리 시간이 증가한다. 네트워크의 규모가 커지는 경우 적합하지 않을 수 있다. Bitcoin-NG는 블록체인의 암호기술에 채굴보다 처리속도가 비교적 빠른 공개키 암호 기술을 결합하여 처리속도와 보안성을 모두 고려한 합의 알고리즘이다. 확장성을 고려하였을 때, 가장 적합하다. 하나의 리더 노드를 선정하는 과정에 모든 노드가 참여함으로서 특정 노드의 독점을 막을 수 있으

며, 공개키 암호 기술을 이용하여 하나의 리더 노드가 여러 개의 신뢰 블록을 생성하는 것이 처리속도를 줄임으로서 보안성과 확장성을 가진 합의 알고리즘이다. 다른 분야로 확장성을 고려하였을 때, 여러 다른 보안 기술과 블록체인 기술을 융합하여 안전성을 고려한 리더 선출을 통해 보안성을 결여 시키지 않도록 여러 개의 신뢰 블록을 생성하는 방법이 효율적일 것이라 사료된다.

5. 결론

블록체인은 P2P 연결에서 신뢰하지 않는 노드들 사이에 신뢰를 합의하는 데이터베이스 시스템이다. P2P 연결을 기반으로 하는 IoT를 비롯한 다양한 분야와의 결합 가능성이 기대되는 기술이다. 합의에 도달하는 시간이 오래 걸리는 등의 문제로 인해 융합에 어려움을 겪고 있다. 하지만 Bitcoin-NG와 같은 보안성의 감소 없이 트랜잭션 처리량을 증가시킬 수 있는 합의 알고리즘을 이용한다면 확장성에 긍정적일 것이라 사료된다. 아직 Bitcoin-NG 또한 완벽한 기술은 아니지만 앞으로 블록체인과 다른 암호 기술의 융합이 시도되다 보면 한계점을 극복할 수 있는 다양한 방법들이 제시될 수 있을 것이라 기대된다.

Acknowledgement

- This study was supported by the Advanced Research Project funded by the SeoulTech(Seoul National University of Science and Technology)

참고문헌

[1] Nakamoto. Satoshi, “Bicoin:A peer-to-peer eletronic cash system”, https://git.dhimmel.com/bitcoin-whitepaper/, Access by Mar. 2020.

[2] 곽현, “블록체인(BlockChain)기술의 산업동향 및 특허동향”, https://www.kiip.re.kr/board/report/view.do?bd_gb=data&bd_cd=4&bd_item=0&po_item_gb=5&po_item_cd=dgb_20&po_no=12351, Access by Mar. 2020.

[3] 이제영, 우청원, “블록체인 기술의 전망과 한계 그리고 시사점”, FUTURE HORIZON, Future Horizon:2018 제38호, 12-15, 2018.

[4] 가사키 나가토, “처음 배우는 블록체인”, 한빛미디어, 2018. (2판)

[5] Sunny. King and Scott. Nadal, “PPcoin:Peer-to-Peer Cryto-Currency with Proof-of-Stake”, https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf, Access by Apr. 2020.

[6] BitFury Group, “Proof of Stake Versus Proof of Work White Paper”, https://www.semanticscholar.org/paper/Proof-of-Stake-versus-Proof-of-Work-White-Paper/69900bac4097a576414f69f1998c11089fb5bb94, Access by Apr. 2020.

[7] 임종철, 유현경, 곽지영, 김선미, “블록체인과 합의 알고리즘”, 전자통신동향분석, 제33권, 1호, 45-56, 2018.

[8] steam, “An incentivized, blockchain-based, public content platform”, https://steem.com/SteemWhitePaper.pdf, Access by Apr. 2020.

[9] Eyal. Ittay, et al, “Bitcoin-NG: A Scalable Blockchain Protocol”, 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), Santa Clara, USA, 2016, pp.45-59.