지분 증명 합의 알고리즘의 발전에 관한 연구

최원석, 우종수, 홍원기
포항공과대학교

{ws4583, woojs, jwkhong}@postech.ac.kr

A Study on Proof-of-Stake Consensus Algorithms

Wonseok Choi[1], Jongsoo Woo[2], James Won-Ki Hong[1]
[1]Department of Computer Science and Engineering, POSTECH
[2]Graduate School of Information Technology, POSTECH

요 약

작업 증명 합의 알고리즘(Proof of Work)은 채굴이라는 혁신적인 방안을 통해 비잔틴 장군 문제와 이중 지불 문제에 대한 해결책을 제시했다. 하지만 점점 경쟁이 치열해지면서 작업 증명 방식의 채굴 난이도는 이에 따라 증가했고, 연산에 높은 수준의 장비와 과도한 양의 전력이 소모되며 큰 에너지 낭비가 발생했다. 지분 증명 합의 알고리즘(Proof of Stake)은 이런 작업 증명 합의 알고리즘의 막대한 에너지 소모에 대한 대안으로써 등장했다. 지분 증명은 검증자들이 보유하고 있는 암호화폐의 지분에 따라 의사결정 권한을 주는 합의 알고리즘들을 통틀어 지칭하는 단어이다. 초기의 지분 증명 합의 알고리즘은 작업 증명 합의 알고리즘과 융합된 형태였으나 순수하게 지분 증명 방식만 사용하는 합의 알고리즘들도 등장했고, 어느 합의 알고리즘이 가장 안전하고 효율적인가에 대한 연구는 계속해서 진행중이다. 최근 이더리움의 창시자인 비탈릭 부테린은 이더리움 2.0 에 대한 계획을 발표했고, 그 핵심 내용 중 하나는 이더리움의 작업 증명에서 지분 증명으로의 전환이었다. 그리고 구체적인 지분 증명의 구현 방식에 대한 내용은 지속적으로 업데이트 되고 있다. 본 논문에서는 초기에 출현한 지분 증명 합의 알고리즘들과 현재 많은 연구가 진행중인 이더리움 2.0 에서의 지분 증명에 대한 분석을 통해 지분 증명 방식이 발전되어 온 과정과 각각의 장단점을 파악하여 앞으로의 지분 증명의 방향성에 대하여 제시하고자 한다.

Ⅰ. 서 론

비트코인 [1]은 2008 년 익명의 개발자 혹은 개발자 그룹인 사토시 나카모토에 의해 처음 공개되었다. 비트코인은 작업 증명(PoW, Proof of Work) 합의 알고리즘을 통하여 비잔틴 장군 문제[2]와 이중 지불 문제[3]를 해결하려 한 최초의 암호화폐이자 가장 유명하고 성공적인 암호화폐이다. 작업 증명 합의 알고리즘에서는 채굴(Mining)이라는 과정을 통해 암호화폐의 거래들이 담긴 블록을 생성한다. 채굴 과정에서 모든 채굴자(Miner)들은 지정된 채굴 난이도에 따라 목표 값보다 작은 해시 값을 생성하는 논스(Nonce) 값을 반복해서 찾는다. 가장 먼저 위 조건에 해당하는 논스 값을 찾은 채굴자는 블록을 생성할 권한을 가지게 되고 블록을 생성한 대가로 일정량의 암호화폐를 얻게 된다.

이러한 작업 증명 방식은 51% 공격[4]을 효과적으로 방지할 수 있기에 긍정적으로 평가받았으나 시간이 지나며 작업 증명 합의 알고리즘에 대한 문제점들도 대두되었다. 가장 큰 문제점은 작업 증명의 채굴 과정에서 오는 막대한 전력 소모였다. 이는 에너지 낭비와 더불어 채굴자들의 단합으로 거대한 채굴 풀(Mining pool)[5]들이 생겨나며 블록 체인의 초기 목표에서 벗어나 오히려 네트워크가 중앙화 되는 현상을 가져왔다.

작업 증명 합의 알고리즘의 이런 문제점을 해결하기 위해 지분 증명(PoS, Proof of Stake)[6] 합의 알고리즘이 등장했다. 지분 증명 합의 알고리즘은 검증자들이 보유한 암호화폐의 지분에 비례하여 의사결정 권한을 가지게 되는 합의 알고리즘들을 통틀어 지칭하는 단어이다. 지분 증명 방식은 작업 증명과 달리 계산 집약적인 작업을 필요로 하지 않기 때문에 작업 증명에서의 막대한 전력 소모 문제를 해결하였고, 작업 증명에 비해 51% 공격을 더욱 효과적으로 막을 수 있다. 하지만, 지분 증명도 여전히 여러 안전성 및 확장성 등의 문제점이 제기되고 있고 이에 대한 연구가 지속적으로 진행중이다.

본 논문에서는 이러한 지분 증명 합의 알고리즘의 출현과 현재 가장 이슈가 되고 있는 이더리움 2.0 [7] 에서의 지분 증명 합의 알고리즘에 대해 분석함으로써 지금까지의 지분 증명의 발전에 대해 정리하고 앞으로 지분 증명 합의 알고리즘이 나아가야할 방향성에 대하여 제시하고자 한다.

Ⅱ. 지분 증명 합의 알고리즘

1. 피어 코인(Peercoin)

피어 코인[6]은 지분 증명 합의 알고리즘을 도입한 최초의 암호화폐로 평가받고 있다. 피어 코인에서는 코인 나이를 도입한 지분 증명 방식과 작업 증명을 융합하여 순수 작업 증명에서의 막대한 에너지 소모 문제를 해결했다. 피어 코인의 지분 증명에서는 피어 코인을 30 일 이상 소유하면 블록 생성에 참여할 수 있게 되고 90 일 이상 소유할 경우 블록 생성에 참여할 확률이 최대가 된다. 코인 나이는 코인을 소유한 기간과 소유한 코인의 수의 곱으로 계산되며 코인 나이가 클수록 블록 생성에 필요한 해시 값을 찾기가 쉬워진다. 작업 증명에서는 블록 생성에 대한 보상이 별도로 존재하지만 지분 증명에서는 거래 수수료외에는 보상이 존재하지 않는다는 것이 큰 차이점이다. 분기가 발생하면 사용된 코인 나이가 큰 체인이 메인 체인으로 선택되며 블록 생성에 성공했다면 일정 비율의 코인을 보상으로 받게 되며 코인 소유 기간이 초기화된다. 피어 코인에서는 이러한 방식의 지분 증명과 작업 증명 방식을 함께 사용하여 에너지 소모를 줄이고 유저들의 참여를 격려한다.

한편, 지분 증명에서는 전체 코인의 51% 이상을 보유해야 51% 공격이 가능하기 때문에 작업 증명에 비해 51% 공격이 더욱 어렵다는 장점 역시 있다. 하지만 피어 코인에서는 코인 보유 기간을 악의적으로 늘려 새로운 체인을 메인 체인으로 만드는 장거리 공격이 가능한 문제점이 있는데 이를 막고자 피어 코인에서는 일정 블록마다 체크포인트를 두어 체크포인트 이전에서는 포크가 발생하지 않도록 했는데 체크포인트는 개발자가 임의로 선정하기 때문에 이것이 피어 코인의 탈중앙화성을 떨어뜨리게 되었다.

2. Nxt

Nxt[8]는 순수하게 지분 증명 방식으로만 구현된 최초의 암호화폐로 평가받고 있다. 피어 코인에서는 지분 증명 방식과 작업 증명 방식을 함께 사용하는 것과 달리 Nxt 에서는 지분 증명 합의 알고리즘만 사용한다. 블록 생성 과정에 참여하기 위해서는 한 계정에 1,440 개의 블록이 생성되는 동안 지분을 걸어 두어야 한다. 이 조건을 만족한 계정은 활성 계정이 되며 블록 생성을 위한 기본 목표 값보다 작은 해시 값을 찾아 내면 블록을 생성할 수 있게 된다. 기본 목표 값은 이전 블록의 목표 값과 생성 시간에 따라 정해진다. 이때, 어느 계정이 블록을 생성할 권리를 갖고, 블록 충돌이 발생했을 때 어느 블록을 유효한 블록으로 처리할 것인가는 이전 블록 생성 후 경과 시간과 계정의 잔액에 영향을 받는다. 즉, 이전 블록 생성 후 오랜 시간이 지날수록, 계정에 많은 코인을 보유할수록 블록을 생성하기 쉬워진다. 모든 계정의 보유 코인은 공개된 정보이기 때문에 이는 다음 블록의 생성자를 예측하기 쉽다는 의미이기도 하다. Nxt 에서는 블록 생성에 대한 대가로 블록 내부의 거래들의 수수료를 가질 수 있다.

하지만, 이 방식에도 문제가 발생할 수 있다. 이는 기본 목표 값이 정해지는 과정에서 발생한다. 기본 목표 값은 이전 블록의 값을 바탕으로 생성되기 때문에 이전 블록의 생성자가 의도적으로 자신에게 유리한 값을 삽입하게 된다면 독점이 발생한다는 것이다. 이는 다른 여러 지분 증명 합의 알고리즘에서도 발생할 수 있는 문제로 이 문제의 가장 핵심이 되는 점은 블록 생성을 위한 랜덤 값의 신뢰성이다.

	피어 코인	Nxt
합의 알고리즘	PoW + PoS	PoS
블록 생성 기준	코인 나이	계정 잔액
블록 생성 참여 조건	코인 나이 30 일 경과	지난 1,440 블록 생성 기간 동안 1000NXT 이상 소유

표 1. 피어 코인 Nxt 비교

3. 이더리움 2.0 (Ethereum 2.0)

비탈릭 부테린은 이더리움 2.0 을 발표하며 작업 증명에서 지분 증명으로의 합의 알고리즘의 전환을 예고했다. 앞서 설명했듯, 이 역시 작업 증명 방식의 막대한 에너지 소모와 중앙화 된 채굴자, 또한 51% 공격 등의 문제를 해결하기 위함이었다. 하지만 지분 증명 합의 알고리즘에도 앞서 소개한 안전성 문제나 랜덤성 문제 외에 다른 문제가 존재한다. 지분 증명은 작업 증명과 같이 증명 과정에 필요한 에너지 소모가 없기 때문에 검증자 입장에서는 모든 체인에 투표하는 것이 이득이고 이로 인해 진정한 합의에 이를 수 없다는 Nothing at stake 문제이다. 이더리움 2.0 에서는 이러한 문제점을 잘못된 체인에 투표했을 때 처벌하는 방식을 이용하여 해결 하고자 한다.

이더리움 2.0 의 발전 과정에서 구체적인 합의 알고리즘에 대해 많은 논의가 있었다. 그 과정에서 작업 증명과 지분 증명이 혼합된 형태로 비탈릭 부테린이 주도하는 Casper FFG(friendly finality gadget)[9]와 순수 지분 증명을 사용하고 블라드 잠피르가 주도하는 Casper CBC(correct by construction)[10]로 나뉘어 졌다.

Casper CBC 는 수학적 증명과 같은 탄탄한 기초부터 시작해서 궁극적으로는 필요한 기능이 모두 구현되고 오류가 없도록 하는 correct by construction 기법을 도입한 합의 알고리즘이다. Casper CBC 는 지분 증명에 관한 연구로부터 시작되었지만 점차 그 영역을 넓혀 일반적인 합의 알고리즘에 대한 연구로 확장되었고 그 중 블록체인에서의 지분 증명을 집중적으로 다루는 연구는 Casper TFG(the friendly GHOST)[11]에서 진행되었다. Casper TFG 에서의 핵심 내용은 지분 증명에서 블록 분기가 발생했을 때의

처리 방법이다. 일반적인 방법으로는 가장 긴 체인, 혹은 가장 많은 지분이 걸린 체인이 메인 체인이 되지만 Casper TFG 에서는 LMD GHOST(latest message driven greedy heaviest observed subtree) 프로토콜을 사용한다. 이 프로토콜에서는 검증자들의 가장 최근의 메시지를 바탕으로 가장 많은 검증자들이 선호하는 체인을 메인 체인으로 삼는다. 이는 가장 긴 체인을 메인 체인으로 삼는 방식과 유사해보이나 잦은 분기가 발생할 때 소수의 검증자가 악의적인 행동을 하더라도 다수의 검증자를 절대 이길 수 없다는 점에서 큰 장점을 가진다.

Casper FFG 는 현재 이더리움의 작업 증명에서 지분 증명으로 넘어가기 위한 단계적인 과정이기에 작업 증명 기반 위에 지분 증명이 추가된 형태로 향후 작업 증명에 해당하는 부분을 바꿔 나가는 계획으로 진행되었다. Casper FFG 는 일반적인 작업 증명 과정에서 일정 블록 수 마다 검사 지점이 존재하고 이 지점에서 지분 증명 기반의 검증자들에 의한 완결성 검증이 존재한다. 일정 블록 수 마다 검증자들은 자신의 지분을 이용해 블록 분기에 투표를 하고, 전체 지분의 2/3 이상이 투표한 블록이 확정되게 된다. 자신이 투표한 블록이 확정되면 그에 따른 보상을 받게 되고, 이중 투표와 같은 악의적인 행동이 발각되면 지분을 몰수당하는 처벌을 받게 된다.

	Casper TFG	FFG
합의 알고리즘	PoS	PoW + PoS
분기 선택 규칙	LMD GHOST	가장 높은 검사 지점을 보유한 체인

표 2. Casper TFG FFG 비교

Gasper[12]는 Casper FFG 와 Casper TFG 에서 사용된 LMD GHOST 프로토콜을 합친 형태로 순수 지분 증명 합의 알고리즘이며 이더리움 2.0 에서 적용할 가장 이상적인 방안으로 최근 새롭게 제안되었다. Gasper 에는 시간을 슬롯으로 구분하며 슬롯 마다 블록이 채워져 있을 수 있고 하나의 epoch 는 여러 개의 슬롯으로 구성되어 있다. Epoch 의 경계는 Casper FFG 에서의 검사 지점으로 사용되며 epoch 마다 검증자들은 슬롯 수만큼의 위원회로 랜덤하게 배정이 되고, 각 슬롯 마다 위원회 중 한 명의 검증자가 블록을 제안하며 나머지 검증인 들은 투표를 한다. 그리고 블록 분기가 발생하면 LMD GHOST 를 약간 변형한 형태인 Hybrid LMD GHOST 프로토콜에 따라 가장 많은 투표를 받은 블록을 선택하게 된다. Gasper 에서는 Casper FFG 와 유사한 방식으로 검증자가 악의적인 행동을 하지 않고 올바른 블록을 생성하는데 성공하면 보상을 받게 되고, 악의적인 행동을 보였다면 지분을 몰수당하는 처벌을 받게 된다.

Ⅲ. 결 론

본 논문에서는 작업 증명 합의 알고리즘의 대안으로 등장한 지분 증명 합의 알고리즘의 발전 과정과 그 응용사례들에 대하여 소개하였다. 지분 증명은 과도한 전력소모라는 작업 증명의 문제점을 해결하기 위해 등장했고, 51% 공격에 대한 문제를 더욱 효과적으로 해결하였다. 하지만, 여전히 51% 공격에 대한 완전한 해결책을 가져다 주진 못하였고, 작업 증명과는 또다른 중앙화성과 불완전한 랜덤성, Nothing at stake 문제 등 많은 새로운 문제가 나타나 이에 관한 연구들이 진행중이다. 새롭게 등장하는 지분 증명 합의 알고리즘들은 작업 증명 등 다른 합의 알고리즘과 융합된 형태들도 여럿 존재하며 저마다 앞의 문제들을 해결하기 위한 독자적인 해결책을 제시하고 있다. 이더리움 2.0 역시 현재 이더리움이 사용하고 있는 작업 증명의 문제점을 해결하기 위해서 합의 알고리즘을 지분 증명으로 전환하려는 계획을 가지고 있다. 이 과정에서 단계적으로 작업 증명과 지분 증명을 함께 사용하지만, 궁극적으로는 지분 증명으로 완전히 대체하고자 한다. 또한, Casper 합의 알고리즘과 GHOST 프로토콜을 이용하여 공평성과 안전성을 더욱 확보하고자 하였으며, Nothing at stake 문제를 위한 처벌 제도 역시 도입할 계획이다.

본 논문에서 소개한 지분 증명 합의 알고리즘들 외에도 세상에는 다양한 종류의 지분 증명 합의 알고리즘들이 존재한다. 그리고 각 알고리즘들은 신뢰성, 보안성, 실용성 등 저마다 각각의 목적을 달성하고자 하며 실질적으로 이러한 모든 특성들을 완벽히 달성하기는 어렵기에 어떤 알고리즘이 더 우월하다고 판별하기 어렵다. 이처럼 앞으로의 지분 증명 합의 알고리즘 역시 각자의 독자적인 목적에 맞게 51% 공격에 대한 좀 더 높은 안전성, 투명하고 편중되지 않은 랜덤한 값의 생성 및 Nothing at stake 문제 등에 대해 기존의 알고리즘보다 더욱 좋은 해결책을 가지고 등장할 것이다. 하지만, 궁극적으로는 이러한 알고리즘들을 다양한 방면에서 활용할 수 있도록 모든 알고리즘들을 아우를 수 있는, 혹은 필요에 따라 전환이 가능한 알고리즘이 필요해질 것이다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구 임(No.2018-0-00539)

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *URL: https://bitcoin.org/bitcoin.pdf (accessed: 15.04. 2020)* (2008).

[2] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine Generals

Problem." *Concurrency: the Works of Leslie Lamport*. 2019. 203-226.

[3] Chohan, Usman W. "The double spending problem and cryptocurrencies." *Available at SSRN 3090174* (2017).

[4] Ye, Congcong, et al. "Analysis of security in blockchain: Case study in 51%-attack detecting." *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 2018.

[5] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *International conference on financial cryptography and data security*. Springer, Berlin, Heidelberg, 2014.

[6] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." *URL: https://decred.org/research/king2012.pdf (accessed: 15.04. 2020)* (2012).

[7] Buterin, Vitalik. "Ethereum 2.0 mauve paper." *Ethereum Developer Conference*. Vol. 2. *URL: https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf (accessed: 15.04. 2020)* (2016).

[8] Popov, Serguei. "A probabilistic analysis of the nxt forging algorithm." *Ledger* 1 (2016): 69-83.

[9] Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." *arXiv preprint arXiv:1710.09437* (2017).

[10] Zamfir, V., et al. "Introducing the minimal CBC Casper family of consensus protocols." *DRAFT v1. URL: https:// github.com/cbc-casper/cbc-casper-paper/blob/master/cbc-casper-paper-draft.pdf (accessed: 15.04. 2020)* (2018).

[11] Zamfir, Vlad. "Introducing casper the friendly ghost." *Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casperfriendly-ghost (accessed: 15.04. 2020)* (2015).

[12] Buterin, Vitalik, et al. "Combining GHOST and Casper." *arXiv preprint arXiv:2003.03052* (2020).