EOS 암호화폐의 블록 생성에 대한 인센티브 분석[1)]

한성호* 안형철* 김광조*

*KAIST 정보보호대학원

Analysis of Incentive for EOS Block Producer

Seongho Han* Hyeongcheol An* Kwangjo Kim*

*Graduate School of Information Security, KAIST.

요 약

비트코인이 제안된 이후 다양한 암호화폐가 개발되었다. EOS는 비트코인의 불필요한 에너지 소모와 낮은 거래 처리량, 그리고 제한된 기능 제공을 극복하기 위해 고안되었다. 합의 방식으로 위임지분증명(DPoS) 방식을 채택한 EOS에서는 개별 블록 생성을 위한 경쟁이 없다. 그러나 EOS의 블록 생성자 선거에서 승리하기 위해서는 성능이 좋은 하드웨어를 갖춰야 하므로 참여 비용이 높다. Itay 등은 블록 생성 보상과 비용의 균형이 깨지면 암호화폐의 보안이 취약해질 우려가 있음을 증명하였다. 따라서 노드가 블록 생성자가 되기 위한 조건을 분석해야 한다. 본 논문에서는 EOS의 블록 생성 보상과 비용을 정량적으로 계산함으로써 블록 생성자가 되기 위한 인센티브를 분석하였다.

I. 서론

2008년 Satoshi Nakamoto에 의해 비트코인[1]이 제안된 이후 다양한 암호화폐가 개발되었다. 비트코인을 포함한 퍼블릭 블록체인은 탈중앙화된 경제시스템 구축을 목표로 한다. 퍼블릭 블록체인에서는 서로 다른 노드들이 동일한 데이터베이스를 유지하기 위해 합의 알고리즘을 사용한다. 비트코인은 작업증명 합의 방식(PoW)을 합의 알고리즘으로 채택하고 있다.

합의 알고리즘이 제대로 기능하기 위해서는 노드들의 자발적 참여가 필수적이다. 그러나 작업증명 합의 방식의 경우 불필요한 에너지 소모가 많[2)]고, 경쟁이 심해지면 채굴 비용이 증가하여 신규 사용자의 진입 장벽이 높아진다는 단점이 있다. Itay 등 [2]은 장래에 비트코인의 채굴 보상이 줄어들면 채굴자들이 블록 생성에 참여하지 않는 시간이 증가할 수 있음을 증명하였다. 노드들이 채굴에 참여하지 않는 시간이 길어지면 블록체인의 보안이 취약해진다.

EOS [3]는 비트코인의 불필요한 에너지 소모와 낮은 거래 처리량, 그리고 제한된 기능 제공을 극복하기 위해 고안된 암호화폐이다. EOS는 비트코인과 달리 합의 방식으로 위임지분증명(DPoS) 방식을 채택하고 있다. 위임지분증명 방식에서는 선거에서 이긴 노드만이 블록 생성에 참여하기 때문에 개별 블록 생성을 위한 경쟁이 없다. 따라서 시간에 따라 블록 생성에 요구되는 연산량이 증가하지 않는다.

그러나 EOS에서는 블록 생성을 위해 블록 생성자 선거에서 승리해야 한다. 선거에서 승리하기 위해서는 성능이 좋은 하드웨어를 갖춰야 하므로 참여 비용이 높다. Itay 등은 블록 생성 보상과 비

1) 본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)

용의 균형이 깨지면 블록 생성에 참여하려는 노드의 숫자가 적어져 암호화폐의 보안이 취약해질 우려가 있다고 주장하였다. 따라서 EOS 노드가 블록 생성자가 되기 위한 인센티브를 분석해볼 필요가 있다.

본 논문에서는 EOS의 블록 생성 보상과 비용을 정량적으로 계산한다. 이를 통해 블록 생성자가 되기 위한 인센티브를 분석한다.

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 EOS 및 위임지분증명(DPoS) 방식에 대하여 설명하고, Ⅲ, Ⅳ장에서는 각각 EOS의 블록 생성 보상과 비용을 분석한다. Ⅴ장에서는 블록 생성 보상과 비용을 고려하여 블록 생성자가 되기 위한 인센티브를 분석한다. 마지막으로 Ⅵ장에서는 결론과 본 논문 성과를 이용한 추후 연구에 대한 가능성을 제시한다.

II. 배경지식

배경지식에서는 EOS와 EOS에서 사용되는 위임지분증명(Delegated Proof-of-Stake, DPoS) [3, 6]에 대하여 설명한다.

2.1 EOS

EOS는 비트코인의 제한된 기능, 불필요한 에너지 소모, 낮은 거래 처리량을 보완하기 위해 개발된 암호화폐다. EOS를 구현한 소프트웨어는 EOS.IO로 탈중앙화 어플리케이션의 수직 및 수평적 확장이 가능하다. EOS.IO는 계정, 인증, 데이터베이스, CPU 스케줄링 등 수많은 기능을 제공한다. 거래 처리량을 초당 수천개로 유지하고, 거래 수수료가 없다는 것이 장점이다.

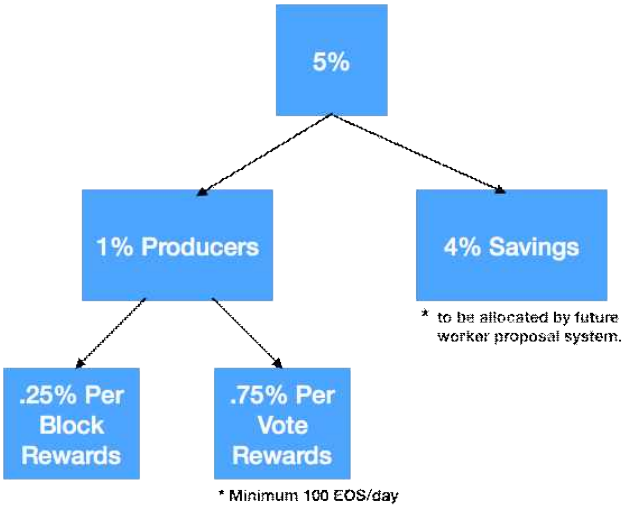
2.2 위임지분증명

위임지분증명 방식은 작업증명 방식과 달리 블록 생성자가 되기 위해선 투표를 거쳐야 한다. EOS에서는 투표를 통해 21명의 블록 생성자(Block Producer, BP)를 선출한다. 선거 방식은 1인 1표가 아니라 1코인 1표 정책을 선택한다. 누구나 블록 생산에 참여할 수 있으며 선거에서 득표 순위가 21위 안에 들 때 블록 생성자가 될 수 있다. 선출된 대표자들은 암호화폐가 정한 계획에 따라 블록을 생성한다. 투표 결과 21위 안에 들지 못했으나 40위 안에 든 사람들에게는 블록 생성후보자의 지위를 부여한다. 장래에는 121위 안에 드는 사람까지 블록 생성후보자의 지위를 부여할 예정이다.

III. EOS 블록 생성자의 블록 생성 보상 체계

EOS 시스템은 2018년 6월 메인넷이 활성화된 시점에 총 10억 개의 토큰을 발행했다. 이후 연간 5%의 인플레이션율에 따라 토큰 발행량이 증가할 예정이다. [그림 1]의 5%는 연간 인플레이션율을 나타낸 것이다.

[그림 1]을 보면 알 수 있듯이 EOS 시스템은 총 EOS 토큰 발행량의 1%를 블록 생성자와 후보자에게 수여한다. 블록 생성자에게 주어지는 보상은 크게 두 종류로 나눠진다. 블록 생성을 수행함으로써 얻는 보상과 투표 득표율에 따라 얻는 보상이 있다. 단, 두 개의 보상을 합쳐 100 EOS 토큰을 초과하지 않으면 어떠한 보상도 주어지지 않는다. 한편 블록 생성후보자는 오직 득표율에 따른 보상만 받을 수 있다. 후보자의 경우 득표율에 따른 보상이 하루에 100 EOS 토큰을 초과하지 않으면 어떠한 보상도 받을 수 없다.



[그림 1] 블록 생성 보상 개념도 [4]

[표 1] EOSUK의 하드웨어 장비 [5]

역할	CPU	RAM	Disc	Expansion
Block Producer Primary	Dual Xeon 3.2GHz 8 Core	128 GB DDR4	512 GB SSD	Yes
Full Node Primary	Dual Xeon 3.2GHz 8 Core	64 GB DDR4	512 GB SSD	Yes

3.1 블록 생성 보상

블록 생성 보상은 블록 생성을 하는 노드에만 주어진다. [그림 1]은 총 EOS 토큰 발행량의 0.25%가 21명의 블록 생성자에게 주어진다는 것을 보여준다. 모든 블록 생성자는 동일한 블록 생성 보상을 받는다. 즉 각각의 블록 생성자에게는 총 EOS 토큰 발행량의 0.0119%가 주어지게 된다. 2018년 6월 기준 EOS의 총 토큰 발행량은 10억이다. 따라서 각각의 블록 생성자들은 1년 동안 119,047 EOS 토큰을 보상으로 받으리라 예측된다. 일별로 보상을 계산해보면 각 블록 생성자들은 하루에 326.16 EOS 토큰을 받을 수 있다. 블록 생성자는 일일 보상이 100 EOS를 초과하므로 항상 보상을 받을 수 있다.

3.2 득표율에 따른 보상

투표 보상에 할당된 총 EOS 토큰은 [그림 1]을 통해 알 수 있듯이 총 EOS 토큰 발행량의 0.75%이다. 각 블록 생성자와 블록 생성후보자는 선거 시 득표한 비율에 따라 보상을 받게 된다. 예를 들어 투표에서 2%의 득표율을 기록한 경우 2018년 기준 1,000,000,000×0.075×0.02인 150,000 EOS 토큰을 받을 수 있다. 이를 하루 평균으로 계산하면 410.96 EOS이다. 즉 득표율이 2%인 경우에는 하루 수익이 100 EOS 토큰을 초과하므로 투표 보상을 받을 수 있다. 블록 생성자로 채택되지 못하고 블록 생성 후보자가 된 경우 투표 보상을 받기 위해서는 득표율이 0.49%를 넘어야 한다. 0.49%라는 임계수치는 총 EOS 토큰 발행량이 변하면 달라질 수 있다.

IV. EOS 블록 생성자의 블록 생성 비용 체계

EOS의 블록 생성에 요구되는 비용으로는 자본 비용과 실행 비용이 있다 [2]. 자본 비용은 CPU, GPU나 RAM같은 하드웨어 장비를 갖추기 위해 소모되는 비용이다. 반면 실행 비용은 실제 블록 생성 시 소모되는 전력에 따른 비용이다.

4.1 자본 비용

EOS 블록 생성자들은 비트코인 채굴자들과 달리 개별 블록 생성을 위해 경쟁하지 않는다. 그러나 EOS 사용자들은 CPU, 네트워크 기능을 블록 생성자로부터 임차하여 사용하기 때문에 블록 생성자에게 높은 하드웨어 수준을 요구한다. 선거 유세 시 유권자들에게 높은 하드웨어 성능을 약속하지 못하는 후보자들은 많은 득표를 할 수 없다. 실제로 [9]는 사용자들이 블록 생성자들에게 고사양의 하드웨어를 갖출 것을 요구한다는 것을 보여주었다. [표 1]은 2018년 11월 기준 득표율이 70~80위에 속한 블록 생성 후보자 EOSUK의 하드웨어 장비를 나타낸 것이다. 이를 통해 개별 블록 생성을 위한 경쟁이 없더라도 블록 생성자가 되기 위한 자본 비용이 높다는 것을 유추할 수 있다.

4.2 실행 비용

블록 생성자가 블록을 생성하고 EOS 사용자에게 편의를 제공하기 위해서는 상시적으로 생성자가 소유한 서버의 전원을 켜놓아야 한다. 그러므로 하루 24시간 내내 전력을 소비할 것으로 예측된다.

V. EOS 블록 생성 인센티브 분석

블록 생성 보상과 블록 생성 비용을 고려하면 블록 생성에 따른 순이익을 구할 수 있다.

순이익 = 총 블록생성보상 − 총 블록생성비용

순이익이 0보다 커야만 자원해서 블록 생성

자가 되려고 할 것이다. 만약 어떤 블록 생성자의 순이익도 0보다 작으면 블록 생성자가 되려는 사람이 없게 되고, 이에 따라 EOS 시스템 자체가 마비된다.

5.1 가상의 상황을 통한 블록 생성 인센티브 측정

가상의 상황을 통하여 블록 생성 인센티브를 측정해본다. 먼저 투표에서 2%를 획득하여 블록 생성자가 되었다고 가정한다. 그리고 하드웨어 장비는 EOSUK와 동일하게 구비했다고 가정한다. 전력 소비는 영국에서 24시간 동안 했다고 가정한다. 순이익은 하루를 기준으로 측정한다.

총 블록 생성 보상은 블록 생성자로써 얻는 블록 생성 보상과 투표로 얻는 보상의 합으로 구할 수 있다. 블록 생성자로써 얻는 블록 생성 보상은 326.16 EOS다. 3장 2절에서 보듯이 투표로 얻는 보상은 410.96 EOS다. 즉 총 블록 생성 보상은 737.12 EOS다. 2018년 11월 기준 EOS를 달러로 환산할 경우 5.73의 교환비를 가지므로 [7] 일일 보상은 4223.6976$이다.

한편 총 블록 생성 비용은 자본 비용과 실행 비용의 합이다. 자본 비용은 Intel CPU Xeon E5-2667v4 8Core 3.20GHz 2200$, RAM 128GB DDR4-2666 2900$, Samsung 850 PRO-512GB 150$다. 이때 하드웨어는 1년간 사용한다고 가정하면 하루에 지출하는 비용은 14.38$다. 실행 비용은 EOS가 1시간에 평균적으로 1.8kW를 사용하므로 [8], 영국 기준 0.22$/kWh [10]의 전기 요금을 대입하면 9.504$이다. 즉 총 블록 생성 비용은 하루에 23.884$이다.

블록 생성 보상과 비용을 이용하여 일일 순이익을 계산해보면 4199.8136$이다. 그러므로 블록 생성자는 계속 현재 상태를 유지하려 할 것이다. 그러나 서버에 필요한 컴퓨터를 100대로 유지하면서, 블록 생성자의 지위를 잃고, 시장 가치가 3$로 하락하게 되면 손해를 볼 가능성이 생긴다. 따라서 EOS의 시장 가격이 적절하게 유지되는 것은 EOS 시스템이 원활하게 돌아가는 데 필수적이다. 또한, 특정 블록 생성자가 득표율을 지나치게 많이 가져가지 않는 것도 EOS 시스템이 제대로 잘 작동하기 위해 필수적이다.

VI. 결론 및 향후 과제

본 논문에서는 EOS의 블록 생성 보상과 비용을 정량적으로 계산함으로써 블록 생성자가 되기 위한 인센티브를 분석하였다. 현재는 21개의 블록 생성자 노드들이 상태를 유지하려는 경제적 유인이 충분하다고 볼 수 있다. 그러나 외부 조건이 변할 경우 블록 생성자 노드들이 현 상태를 유지하지 않을 가능성도 있다.

향후 연구에서는 블록 생성 후보자들 사이의 경쟁에 따른 블록 생성 인센티브를 분석한다. 그리고 경쟁 조건에 따라서 EOS 시스템이 어떠한 방식으로 작동할지 예측해본다.

[참고문헌]

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

[2] Tsabary, Itay, and Ittay Eyal. "The Gap Game." Proceedings of the 11th ACM International Systems and Storage Conference. ACM, 2018.

[3] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[4] https://medium.com/eosio/introducing-eosio-dawn-4-0-f738c552879

[5] https://eosuk.io/eos-block-producer-technical-specifications/

[6] Larimer, Daniel. "Delegated proof-of-stake (dpos)" Bitshare whitepaper, 2014.

[7] https://coinmarketcap.com/

[8] https://medium.com/genereos/eos-energy-consumption-vs-bitcoin-and-ethereum-2d1bb31ed72f

[9] https://steemit.com/eos/@blockmaker/eos-io-block-producer-guesstimated-specsl

[10] https://en.wikipedia.org/wiki/Electricity_pricing