Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.303

비트코인 채굴 수익성 모델 및 분석*

이 진 우,[1†] 조 국 래,[2] 염 대 현[1‡]
[1]명지대학교, [2]대구경북과학기술원

Bitcoin Mining Profitability Model and Analysis*

Jinwoo Lee,[1†] Kookrae Cho,[2] Dae Hyun Yum[1‡]
[1]Myongji University, [2]DGIST

요 약

비트코인은 2009년 사토시 나카모토가 제안한 암호 화폐로 중앙 기관 없이 통화가 발행, 관리되는 분산 합의 구조를 가지고 있다. 채굴은 이러한 분산 합의 구조의 중추를 담당하는 작업으로 대기 중인 비트코인의 거래를 블록화하여 비트코인의 블록체인(장부)에 포함시키는 역할을 한다. 블록의 생성에는 컴퓨팅 자원이 필요하기 때문에, 채굴을 담당하는 채굴자에게 보상으로 비트코인이 지급되며, 이 보상을 통해 새로운 비트코인이 발급된다. 비트코인은 2100만개 까지만 발행할 수 있도록 설계되었으며, 인플레이션에 대비하기 위해 채굴 과정에 반감기라는 개념이 도입되었다. 2009년에 50 BTC이었던 보상은 현재 12.5 BTC인 상태이나 채굴 보상의 실제 가치는 더욱 늘어났다. 이는 2017년 1월 12일 기준 1 BTC당 924,000원이던 비트코인이 2017년 12월 10일 기준 16,103,306원이 되어 실질 보상액을 증가시켰기 때문이다. 가격 상승으로 인해 신규 채굴자가 지속적으로 유입되고 있음에도 채굴이 실제로 어느 정도 수익성이 있는지에 대한 연구는 미비한 상태이다. 본 논문에서는 비트코인의 채굴 구조를 살펴보고 비트코인의 채굴에 어느 정도의 수익성을 기대할 수 있는지를 살펴보고자 한다.

ABSTRACT

Bitcoin (BTC) is a cryptocurrency proposed by Satoshi Nakamoto in 2009. Bitcoin makes its transactions with no central authorities. This decentralization is accomplished with its mining, which is an operation that makes people compete to solve math puzzles to include new transactions into block, and eventually block chains (ledger) of bitcoin. Because miners need to solve a complex puzzles, they need a lot of computing resources. In return for miners' resources, bitcoin network gives newly minted bitcoins as a reward to miners when they succeed in mining. To prevent inflation, the reward is halved every 4 years. For example, in 2009 block reward was 50 BTC, but today, the block reward is 12.5 BTC. On the other hands, exchange rate for bitcoin and Korean Won (KRW) changed drastically from 924,000 KRW/BTC (January 12th, 2017) to 16,103,306 KRW/BTC (December 10th, 2017), which made mining more attractive. However, there are no rigorous researches on the profitability of bitcoin mining. In this paper, we evaluate the profitability of bitcoin mining.

Keywords: Cryptocurrency, Bitcoin, Mining, Profitability

I. 서 론

비트코인(Bitcoin, BTC)은 2009년 사토시 나카모토(Satoshi Nakamoto)가 제안한 암호 화폐로 중앙 기관의 통제가 없는 분산 구조를 형성하여 네트워크가 연결되어 있다면 서로 신뢰하고 거래할 수 있

Received(12. 20. 2017), Modified(03. 09. 2018), Accepted(03. 10. 2018)
* 본 연구는 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원(NRF-2017R1D1A1B03031413)을 받아 수행되었으며, 미래창조과학부에서 지원하는 DGIST 기관고유사업(17-BT-01)에 의해 수행되었습니다.
† 주저자, jinwoo.plum@gmail.com
‡ 교신저자, dhyum@mju.ac.kr(Corresponding author)

는 특징을 가지고 있다. 비트코인은 지속적인 성장을 거듭하여 현재는 가상화폐 거래소 중 하나인 빗썸(bithumb)에서만 24시간 내 거래량이 약 5천억 원이 될 정도에 이르렀다[1]. 비트코인의 가치가 증가함에 따라 그 수요도 증가하였는데 비트코인을 취득할 수 있는 방법은 크게 가상화폐 거래소 등을 통해 현금으로 비트코인을 구매하는 것과 채굴이라는 과정을 통해 새로이 생산된 비트코인을 얻는 방법이 있다.

비트코인의 신뢰성은 블록체인이라고 불리는 장부에 기반을 둔다. 블록체인의 기본 요소가 되는 블록의 생성에는 컴퓨팅 자원이 필요하기 때문에, 채굴을 담당하는 채굴자에게 보상으로 비트코인이 지급된다. 하나의 블록에는 다수의 거래(트랜잭션)가 포함되는데, 비트코인 블록의 첫 번째 거래는 채굴자에게 블록 생성에 대한 보상을 주기 위해 할당된 것이다. 이를 코인베이스 거래라고 한다.

비트코인의 발행 총량은 21,000,000 BTC로 그 수가 정해져 있다. 채굴을 통해 블록이 생성될 때마다 보상으로 새 비트코인이 생성되는데 이 보상값은 시간에 따라 줄어들도록 만들어져 있다. 이는 발행 총량을 제한하기 위한 방식이다. 2009년에 50 BTC 이었던 채굴 보상은 2012년에 25 BTC가 되었고 2016년에는 12.5 BTC가 되었다. 채굴 보상이 0이 되는 시점은 2140년이다. 채굴 보상이 0이 되더라도 채굴을 통해 비트코인을 얻을 수 없는 것은 아니다. 비트코인의 이용자들이 자신의 거래가 블록에 빠르게 포함되도록 하기 위해 채굴자에게 거래마다 수수료를 지급하기 때문이다. 2017년 12월 10일 기준 블록 당 수수료는 블록당 보상인 12.5 BTC보다 적은 2.8 BTC 수준이다[2]. 동시기 기준 1 BTC의 가격이 16,103,306원[1] 이기 때문에 블록 하나를 채굴했을 때 얻을 수 있는 수익은 15.3 BTC, 한화로 약 246,380,581원이 된다.

채굴 보상 반감기의 존재에도 불구하고 블록 하나를 채굴했을 때 얻을 수 있는 실제 수익은 증가하고 있는데 이는 반감기로 인해 줄어드는 보상보다 1 BTC의 가격 증가 폭이 크기 때문이다. 2017년 1월 12일 기준 1 BTC당 924,000원이던 비트코인 가격은 2017년 12월 10일 기준 16,103,306원에 달하고 있다[1]. 이러한 이유로 인해 채굴의 수요가 증가하고 있으나 채굴이 실제로 어느 정도의 수익성을 보이는지에 대한 연구는 미비한 실정이다. 채굴에는 많은 양의 컴퓨팅 자원이 필요하기 때문에 일정 수준의 자본 투자가 필요하다. 따라서 자본을 투자할만한 잠재성이 비트코인 채굴에 있는지 확인하기 위한 연구가 필요하다. 본 논문에서는 비트코인의 채굴 구조를 살펴보고, 채굴을 실제로 행할 경우 어느 정도의 수익성을 기대할 수 있는지를 정리한다.

II. 관련 연구

중앙 기관 없는 전자 통화로서의 비트코인은 사토시 나카모토에 의해 제안되었다[3]. 비트코인 채굴에 대해서는 "이기적인 채굴" 과 같은 가능한 공격 방식에 대한 연구[4], 채굴 풀(채굴자들의 모임)에 대한 DDoS 공격 분석[5] 등 이론적인 접근이 주를 이루었다. 국내에서도 채굴에 대한 다수의 연구가 이루어졌으나 이 또한 이기적인 채굴[6]이나 비트코인 거래의 법적 쟁점[7], 비트코인의 취약점 연구[8]와 같이 주로 이론적, 법리적인 접근이 많았다. 본 논문은 채굴의 수익성에 대한 내용을 다룬다.

III. 채굴 수익

개인의 월별 채굴 순이익 P_{net}은 월별 채굴 이익 P_{earn}에서 월별 전기 요금 C_{elec}과 기계비용 C_{device}, 그리고 채굴 풀 수수료 C_{pool}을 차감한 것으로 나타낼 수 있다. 전기 요금은 채굴 기계를 사용함에 따라 발생하는 비용이고, 기계비용은 채굴 기계를 구매하기 위해 사용한 비용이다. 채굴 풀 수수료는 채굴 풀을 이용하기 위해 내는 수수료인데, 개인이 채굴을 할 경우 긴 기간 동안 하나의 블록도 채굴하지 못할 확률이 높기 때문에 자신의 컴퓨팅 자원을 풀에 제공함으로써 채굴에 성공하지 못하더라도 채굴 풀에 제공한 컴퓨팅 자원에 비례하는 보상을 받을 수 있다. 다만 이를 위해 일반적으로 채굴 풀에 일정 금액의 수수료를 지불해야 한다.

정리하면 $P_{net} = P_{earn} - (C_{elec} + C_{device} + C_{pool})$와 같다. 채굴 이익 P_{earn}은 채굴에 성공하여 얻는 보상 및 수수료(BTC)에 환율(KRW/BTC)을 곱하여 얻을 수 있다. 채굴 이익의 계산을 위해 우선 비트코인의 채굴이 어떻게 이루어지는지를 알아본다.

채굴은 네트워크에 전송된 거래를 모아 하나의 블록 후보를 만든 뒤, 그 블록에 추가할 올바른 해시값을 찾아내어 블록을 완전하게 만든 뒤(블록 생성) 비트코인의 블록체인에 추가시키는 과정으로 이루어진다[9]. 블록을 생성한 모든 채굴자가 보상을 받는

것이 아니라 가장 빠르게 블록을 생성하여 이를 다수로부터 인정받은 한 명의 채굴자만이 보상을 받는다. 따라서 블록을 빠르게 생성하여 블록체인에 추가시키는 것이 중요한데, 이 과정 중 해시 값을 찾는 과정에 가장 많은 컴퓨팅 자원이 소모된다. 채굴에 성공할 수 있는 확률은 전체 채굴자의 해시 능력에 대한 개인의 해시 능력의 비율과 같다. 해시 능력은 일반적으로 해시율(hash rate)을 통해 수치화되며 초당 1테라(10^{12})번의 해시 연산을 할 수 있는 기기는 해시율 1TH/s가 된다.

비트코인에 존재하는 모든 채굴자의 해시율을 H_{tot}로 표기하고, 개인의 해시율을 H_{indv}로 표기하면 월별 채굴 이익 P_{earn}은 다음과 같이 나타내어진다.

$$\begin{aligned} P_{earn} &= (H_{indv}/H_{tot}) \cdot (B_{reward}+B_{fee}) \\ &\quad \cdot 30 \cdot (24 \cdot 60 \cdot 60/600) \cdot E_{rate} \\ &= (H_{indv}/H_{tot}) \cdot (B_{reward}+B_{fee}) \cdot 4{,}320 \cdot E_{rate} \end{aligned} \quad (1)$$

B_{reward}는 채굴 보상인 12.5 BTC이며, B_{fee}는 채굴을 통해 받을 수 있는 수수료로 비트코인 네트워크의 상태에 따라 변화한다. 평균 600초마다 한번 채굴이 이루어지므로 한 달 채굴 횟수는 30 • 24 • 60 • 60/600인 4,320번과 같다. 채굴한 비트코인의 가치는 실물화폐와의 교환율에 따라 변하게 되며, 이때 교환율은 E_{rate}로 표기한다. 월별 순이익 $P_{net} = P_{earn} - (C_{elec}+C_{device}+C_{pool})$에서 월별 전기 요금 C_{elec}은 전기요금을 통해, 기계비용 C_{device}는 기계의 가격을 통해, C_{pool}은 사용할 풀 서비스 업체의 정책을 통해 계산할 수 있다.

정리하면 P_{net}은 수식 (2)와 같이 계산된다.

$$\begin{aligned} P_{net} &= (H_{indv}/H_{tot}) \cdot (B_{reward}+B_{fee}) \cdot 4{,}320 \cdot E_{rate} \\ &\quad - (C_{elec}+C_{device}+C_{pool}) \end{aligned} \quad (2)$$

IV. 채굴 수익의 변수

이 장에서는 수식 (2)의 각 변수 값을 설정하는 방법을 설명한다.

4.1 H_{indv}

개인의 해시율은 개인이 사용할 기기에 따라 달라진다. 초기 비트코인 채굴은 개인용 컴퓨터로도 가능했으나 H_{tot}의 증가로 인해 비트코인 채굴의 난이도가 증가하여 현재는 개인용 컴퓨터로 수십 년을 계산하여도 한 블록의 채굴조차 쉽지 않다. 2017년 기준 최신 그래픽카드인 라데온 R9 209X를 8대 사용하여도 해시율은 1.12 GH/s 정도인데[11] 개인 채굴 환경에서 사용되고 있는 ASIC(Application Specific Integrated Circuit) 기반 비트코인 채굴기인 Bitmain사의 Antminer S9를 사용하면 해시율 13,500 GH/s로 채굴이 가능하다. Antminer S9의 가격은 1,415달러(약 154만원)로 그래픽카드를 이용한 채굴과 가격차가 크지 않음에도 채굴 성능은 약 1만 배가 된다.

따라서 현재 H_{indv}는 ASIC를 이용할 때의 수치로 설정하는 것이 타당하다. 채굴에 널리 사용되고 있는 Bitmain사의 비트코인 채굴기 해시율 정보는 판매 페이지에 게시되어 있다[12]. 본 논문에서는 H_{indv}를 Antminer S9의 해시율인 13,500 GH/s로 설정한다.

4.2 B_{reward}, B_{fee}

현재 B_{reward}는 12.5 BTC이다. 이 값은 2020년에 절반으로 감소하므로[13], 2017년 현재는 12.5 BTC의 고정된 값으로 볼 수 있다. B_{fee}는 변동이 있는 값이지만 그 폭이 크지 않고, 2016년 12월부터 2017년 12월까지 최저 약 0.5 BTC에서 최고 약 7.3 BTC정도였다[2]. 이 추이는 Fig. 1.에서 확인할 수 있다. 본 논문에서는 B_{fee}를 2016년 12월부터 2017년 12월까지의 평균값인 1.6 BTC의

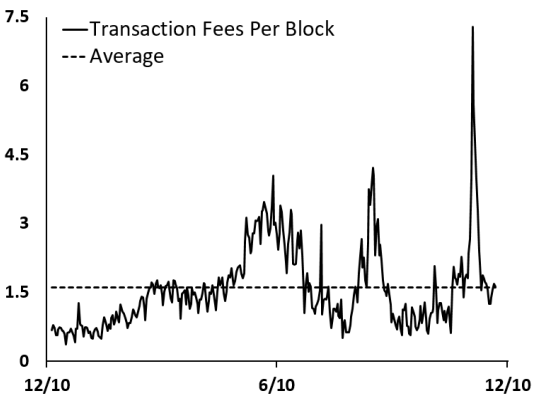

Fig. 1. Value of B_{fee} from Dec. 2016 to Dec. 2017[2]

고정된 값으로 둔다.

4.3 C_{elec}, C_{device}, C_{pool}

C_{elec}은 한국전력공사에서 제공하는 전기요금계산기를 통해 계산할 수 있다[10]. 전기 소모량은 사용하는 비트코인 채굴기에 따라 달라지며, 본 논문에서는 Antminer S9 채굴기를 사용하는 것으로 가정하므로 전기 소모량은 1,323 W가 된다. 일반용(갑)I 전기를 이용할 경우 Antminer S9의 한 달 사용 시 전기 요금은 133,240원이 된다.

C_{device}는 Antminer S9의 가격인 1,415달러를 사용 개월 수로 나눈 값이다. C_{pool}은 채굴 풀 서비스를 통해 안정적으로 수익을 얻을 수 있는 대신에 풀 서비스 업체에 내는 비용이다. C_{pool}은 월별 채굴 이익 P_{earn}에 대해 0%에서 3% 정도의 값을 가진다[14]. 본 논문에서는 2017년 한 해 동안 가장 많이 이용된 풀 서비스 업체인 AntPool의 1%를 C_{pool}로 가정한다[15].

4.4 H_{tot}

비트코인 네트워크의 전체 해시율인 H_{tot}는 비트코인 네트워크가 성장함에 따라 지속적으로 증가해 왔다. 이 증가 추세는 정확하게 수치화하기 어려우나, 2016년 12월부터 2017년 12월에 한하여 Fig. 2와 같이 선형적인 증가 추세를 보이고 있다.

2016년 12월의 H_{tot}를 2,000,000 TH/s로 두고 2017년 12월의 H_{tot}를 12,000,000 TH/s로 둔다면 2017년 12월을 원점으로 두었을 때 n개월이 경과하였을 시점의 H_{tot}는 약 12,000,000 TH/s + n × 830,000 TH/s가 된다. 여기서 830,000 TH/s는 (12,000,000 - 2,000,000)/12의 결과인 833,333 TH/s 의 근사값이다.

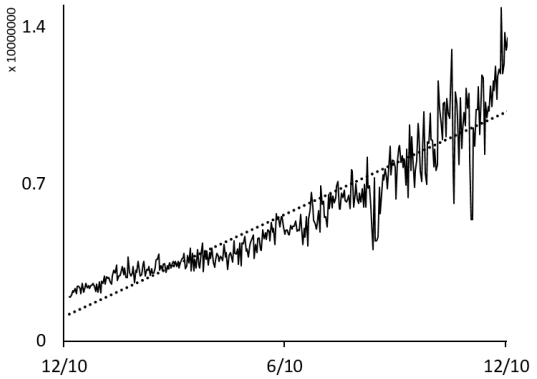

Fig. 2. Value of H_{tot} from Dec. 2016 to Dec. 2017[16]

4.5 E_{rate}

비트코인 환율 E_{rate}는 변수 중에서 가장 예측하기 어려운 값이다. 원화 거래가 가능한 거래소인 Bithumb을 기준으로 2013년 6월 1일에 143,345원이었던 1BTC는 2017년 12월 10일 기준으로 16,103,306원에 달한다[1]. 반대로 E_{rate}는 2017년 11월 29일 19:20 UTC(협정 세계시)와 19:30 UTC간의 10분 만에 1000달러 이상 급락하기도 하였다[17]. 비트코인 시세의 급격한 변화는 Fig. 3.을 통해 확인할 수 있다. 유동성이 이와 같이 크기 때문에 E_{rate}를 예측하는 것은 어려우므로, 본 논문에서는 E_{rate}가 (1)현재 값을 유지할 경우, (2)75% 하락할 경우, (3)100% 상승할 경우의 세 가지로 나누어 분석한다. 12월 10일의 E_{rate}는 약 16,000,000원/BTC이므로, 현재 값을 유지할 경우의 E_{rate}는 16, 000,000원/BTC이고, 75% 하락할 경우의 E_{rate}는 4,000,000원/BTC, 그리고 100% 상승할 경우의 E_{rate}는 32,000,000원/BTC와 같다.

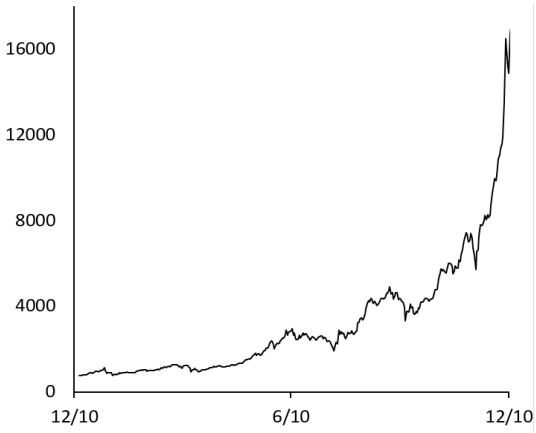

Fig. 3. Value of 1BTC as USD from Dec. 2016 to Dec. 2017[18]

V. 채굴 수익 계산 결과

구한 값들을 수식 (2)에 넣어 계산하면 비트코인 채굴로 인한 수익을 계산할 수 있다. 채굴 기간(월)

에 따른 적분 변수를 m이라고 하고 $P_{net}(n)$을 n개월 채굴 시의 순이익이라 하면 $P_{net}(n)$은 다음과 같이 정리된다. 이 때, C_{elec}은 133,240원인 값을 $1.3 \cdot 10^5$원으로 근사하였고, 채굴 기기의 가격인 1,415달러는 $1.5 \cdot 10^6$원으로 근사하였다.

$$
\begin{aligned}
P_{net}(n) &= \int_{m=0}^{n} (H_{indv}/H_{tot})(B_{reward}+B_{fee})4{,}320E_{rate} \\
&\quad - (C_{elec}+C_{pool}+C_{device})\,dm \\
&= \int_{m=0}^{n} ((H_{indv}/H_{tot})(B_{reward}+B_{fee})4{,}320 \cdot 0.99E_{rate} - C_{elec})\,dm \\
&\quad - 1.5 \cdot 10^6 \\
&= \int_{m=0}^{n} \left(\frac{13.5 \cdot 14.1 \cdot 4320}{1.2 \cdot 10^7 + 8.3 \cdot 10^5 m}0.99E_{rate} \right. \\
&\quad \left. - 1.3 \cdot 10^5\right)dm - 1.5 \cdot 10^6 \\
&= 0.98E_{rate}\int_{m=0}^{n} \frac{1}{m+14}dm \\
&\quad - 1.3n10^5 - 1.5 \cdot 10^6 \\
&= 0.98E_{rate}\ln\frac{n+14}{14} \\
&\quad - 1.3n10^5 - 1.5 \cdot 10^6
\end{aligned}
\tag{3}
$$

n이 0에서 12 사이일 때, 즉 1년 동안 채굴을 진행할 경우에 대해 E_{rate}를 16,000,000원/BTC, 4,000,000원/BTC, 32,000,000원/BTC 으로 설정하면 수식 (3)의 계산 값은 Fig. 4.와 같다.

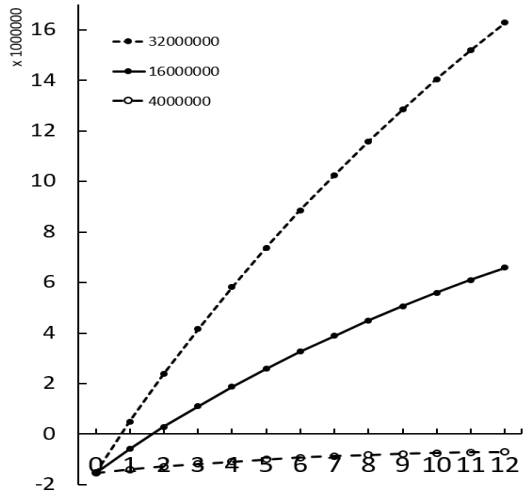

Fig. 4. $P_{net}(n)$, where n is from 0 to 12 and E_{rate} is 4,000,000, 16,000,000, and 32,000,000

Fig. 4.의 시사점은 다음과 같다. 먼저 E_{rate}의 값과 관계없이 시간이 지남에 따라 $P_{net}(n)$이 점점 커지는 것을 확인할 수 있다. 단 $P_{net}(n)$의 기울기는 E_{rate}에 크게 의존하며, E_{rate}가 4,000,000원/BTC인 경우에 12개월이 지나도 $P_{net}(n)$이 0을 넘지 못함을 확인할 수 있다. E_{rate}가 16,000,000원/BTC인 경우 약 2개월 만에 $P_{net}(n)$이 0이 되며, E_{rate}가 32,000,000원/BTC인 경우 약 1개월 만에 $P_{net}(n)$이 0이 된다.

다음으로 $P_{net}(n)$의 기울기가 시간이 지남에 따라 점점 감소하는 것이 확인된다. 즉, $\frac{d}{dn}P_{net}(n)$은 감소함수이다. E_{rate}가 4,000,000원/BTC인 경우 첫 한 달 간의 수익은 약 14만원이나, 마지막 달의 수익은 약 2.2만원이 된다. E_{rate}가 16,000,000원/BTC인 경우에는 약 95만원으로부터 약 48만원으로 감소하며, E_{rate}가 32,000,000원/BTC인 경우에는 약 200만원으로부터 100만원으로 감소한다. 이러한 $P_{net}(n)$의 기울기의 큰 감소는 H_{tot}가 꾸준히 증가하는 것이 원인이며, 이를 상쇄하기 위해서는 주기적인 투자를 통해 H_{indv}를 증가시켜야 한다.

Fig. 5.는 초기비용을 n개월 만에 회수하기 위한 최소 E_{rate}값을 나타낸다. 즉, n개월 만에 $P_{net}(n)$을 0으로 만들 수 있는 E_{rate}를 나타낸다. Fig. 4.에서 확인할 수 있듯이 $P_{net}(n)$의 기울기가 시간이

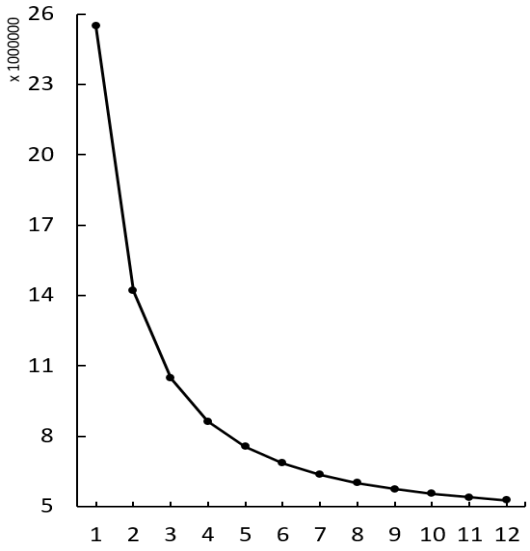

Fig. 5. E_{rate} (y axis) for $P_{net}(n) = 0$ in n months (x axis)

지남에 따라 감소하기 때문에 $P_{net}(n)$을 0으로 만들 수 있는 E_{rate}는 n이 증가함에 따라 수렴하는 경향을 보인다. 12개월간의 채굴을 통해 초기비용을 회수하려면 E_{rate}가 약 5,300,000원/BTC가 되어야 한다. 즉, E_{rate}가 5,300,000원/BTC보다 작은 경우 12개월이 되어도 초기비용을 회수할 수 없기 때문에 0보다 작은 $P_{net}(n)$을 얻어 손해를 보게 된다.

비트코인 환율 E_{rate}가 5,500,000원/BTC일 경우 $P_{net}(12) > 0$이므로 12개월이 되면 초기비용을 회수할 수 있지만, 초기비용을 회수한 이후로 계속 수익이 발생하는 것은 아니다. E_{rate}가 5,500,000원/BTC를 유지한다면 $P_{net}(48)=0$ 또한 성립하므로 12개월이 지난 이후의 특정 시점에서부터는 채굴을 통해 얻을 수 있는 이익이 전기 요금 등의 지출보다 적어진다는 것을 알 수 있다. 따라서 장기적으로 채굴을 통한 수익을 유지하려면 주기적인 채굴 기기에 대한 투자도 고려되어야 할 것이다.

VI. 결 론

Fig. 4.를 통해 2017년 12월 10일의 E_{rate}(약 16,000,000원/BTC)가 유지된다면 2개월이면 초기비용을 회수할 수 있으며 3~4개월이면 초기비용만큼의 수익을 발생시킬 수 있음을 확인할 수 있다. 구체적으로 계산할 경우 채굴 기기(Antminer S9)를 한 대 구입하여 154만원을 투자한다면 4개월 후에는 초기비용인 154만원에 더해 약 187만원의 이익을 얻을 수 있다. Fig. 5.를 통해 E_{rate}가 약 5,300,000원/BTC가 되면 12개월간의 채굴을 통해 초기비용을 회수할 수 있음을 확인할 수 있다.

그러나 비트코인의 가치는 변동이 극심하다. 따라서 비트코인이 현재의 가치를 유지하리라고 확신하기는 어려운 상황이기 때문에 실제로 비트코인 채굴을 계획 중이라면 본 논문이 정리한 각 요소의 현재 값과 미래 값을 면밀하게 검토, 예측하여야 할 것이다.

본 논문을 통해 2017년 12월 현재를 기준으로 비트코인의 채굴이 우수한 수익성을 가지고 있음을 확인하였다. 비트코인의 실제 가치가 현재와 같거나 또는 증가한다면 비트코인 채굴은 기기 비용과 전기료를 모두 고려하더라도 상당히 수익성이 좋은 편이다. 하지만, 비트코인 가격이 급락한다면 비트코인 채굴 수익성도 급격히 감소하여 비트코인 네트워크에 참여하는 채굴자의 수가 감소할 것으로 보이며 이는 비트코인 네트워크의 안전도에 악영향을 끼칠 것으로 예상된다. 본격적인 비트코인 채굴의 역사는 매우 짧기 때문에 채굴 기기의 발달, 비트코인 가격 변동, 채굴풀의 변화, 거래 수수료 변화 등을 고려한 비트코인 채굴의 수익성에 대한 연구가 지속적으로 수행되어야 할 것으로 판단된다.

References

[1] BTC KoreaCom Corporation, "Bithumb," https://www.bithumb.com/, Dec. 2017

[2] SmartBit, "Bitcoin Chart - Transaction Fee," https://www.smartbit.com.au/charts/transaction-fees-per-block, Dec. 2017

[3] S. Nakamoto, "Bitcoin: A Peer-to-peer electronic cash system," https://www.bitcoin.org/bitcoin.pdf, Nov. 2008

[4] A. Sapirshtein and Y. Sompolinsky, "Optimal selfish mining strategies in bitcoin," International Conference on Financial Cryptography and Data Security, pp. 515-532, May 2017

[5] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," International Conference on Financial Cryptography and Data Security, pp. 72-86, Oct. 2014

[6] Sohee Kim, Jiyeon Yang, and Yoonjeong Kim, "A study on the selfish mining of block chain," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 422-423, Nov. 2015

[7] Hongki Kim, "Bitcoin regulation: legal and regulatory issues of the virtual currency system," The Korean Journal of Securities Law, 15(3), pp. 377-431, Dec. 2014

[8] Seogu Kang, Hyungjoon Bae, Seonghyeon Lim, and Youngsook Lee, "A study on the vulnerability and countermeasures of bitcoin," Proceedings of the Korean Society of Computer Information Conference, pp. 124-127, Jul. 2017

[9] P. Ankalkoti and S.G. Santosh, "A relative study on bitcoin mining," Imperial Journal of Interdisciplinary Research, vol. 3, no. 5, pp. 1757-1761, May 2017
[10] KESPO, "Electricity bill calculator," http://cyber.kepco.co.kr/ckepco/front/jsp/CY/J/A/CYJAPP000.jsp, Dec. 2017
[11] Epixoip, "World's first 8x R9 290X ocl hashcat benchmark," https://gist.github.com/epixoip/8171031, Dec. 2017
[12] Bitmain, "ASIC bitcoin mining hardware," http://www.bitmain.com/, Dec. 2017
[13] Bitcoin Clock, "Bitcoin clock," http://bitcoinclock.com/, Dec. 2017
[14] J. Tuwiner, "Bitcoin mining pools," https://www.buybitcoinworldwide.com/mining/pools/, Dec. 2017
[15] BTC.com, "Pool stats - BTC.com," https://btc.com/stats/pool?pool_mode=year, Dec. 2017
[16] Blockchain, "Hash rate - blockchain," https://blockchain.info/ko/charts/hash-rate?timespan=1year, Dec. 2017
[17] P. Rizzo, "Bitcoin price falls $1,000 in minutes to drop below $10k," https://www.coindesk.com/bitcoin-price-falls-1000-minutes-erase-24-hour-gains, Nov. 2017
[18] Blockchain, "Bitcoin - USD/BTC," https://blockchain.info/ko/charts/market-price?timespan=1year, Dec. 2017

〈저자소개〉

이 진 우 (Jinwoo Lee) 정회원
2011년 2월: 포항공과대학교 전자전기공학과 학사
2017년 2월: 포항공과대학교 전자전기공학과 박사
2017년 3월~2018년 2월: 대구경북과학기술원 동반진단연구실 박사후연구원
2018년 3월~현재: 명지대학교 정보보안연구실 박사후연구원
〈관심분야〉 정보보호, 암호 구현, IT융합

조 국 래 (Kookrae Cho) 정회원
2004년 2월: 부경대학교 전자컴퓨터공학부 학사
2006년 2월: 포항공과대학교 정보통신학과 석사
2006년 2월~현재: DGIST 융합연구원 동반진단연구실 선임연구원
〈관심분야〉 공개키 암호, IoT 암호프로토콜, 블록체인 기반의 의료데이터 보안

염 대 현 (Dae Hyun Yum) 종신회원
1998년 2월: 포항공과대학교 전자전기공학과 학사
2000년 2월: 포항공과대학교 전자전기공학과 석사
2006년 2월: 포항공과대학교 전자전기공학과 박사
2006년 3월~2012월 8월: 포항공과대학교 박사후연구원 및 연구교수
2012년 9월~현재: 명지대학교 정보통신공학과 부교수
〈관심분야〉 공개키 암호, 암호프로토콜, 블록체인, 암호화폐