정 보 보 호 학 회 지
제28권 제3호, 2018. 6

신규 참여자의 형평성 향상을 위한 블록체인에서의 새로운 증명 방식 연구: Proof-of-Probability

김 성 민*, 김 경 선**, 김 중 헌***

요 약

최근 블록체인 기술을 응용한 가상화폐에 대한 관심이 높아지면서 자본금이 많지 않은 사람들도 블록체인 네트워크에 참여하기 시작했다. 가장 유명한 가상화폐인 비트코인이 채택한 PoW 방식은 고성능 하드웨어의 과열된 열풍을 불어왔고 PoS 방식은 기존 지분이 많은 참여자들이 많이 존재하여 소수의 자본금을 가진 신규 참여자들이 네트워크에 새로 참여하기 어려운 환경이다. 따라서 본 논문에서는 기존 블록체인 증명방식인 PoW, PoS 방식보다 네트워크 참여를 위한 자본금이 적고 신규로 참여하더라도 리스크가 적은 PoP(Proof-of-Probability) 방식을 소개한다. PoP 방식은 블록을 생성할 시 실제 암호화된 해쉬와 수많은 가짜 해쉬를 각 노드들이 정렬하여 진짜 해쉬를 복호화하여 찾은 노드가 블록을 생성하는 방식이다. 또한 1개의 해쉬를 복호화하여 검증받을 때 1분의 대기시간을 두어 과열된 컴퓨팅파워 경쟁을 제한한다. 지분(Stake)이 많을수록 블록을 생성할 확률은 높아지지만 이는 PoS 방식처럼 절대적이지 않다. 이 방식을 이용한다면 지분을 많이 가진 유효성 검증자(Validators)에 의한 집중화를 피하며 블록체인 네트워크에 참여하려는 진입장벽도 낮출 수 있을 것 이다.

Ⅰ. 서 론

블록체인 기술의 첫 사례인 비트코인의 성공에 힘입어 가상화폐에 대한 많은 관심이 나타나고 있다. 이를 뒷받침하는 것이 바로 시가 총액과 거래량이다. 비트코인의 시가 총액은 1,700억 달러로 예상되고 하루에 확인된 거래량은 375,000개 이상이다.(2017년 12월 기준) 따라서 사람들은 비트코인을 포함한 가상화폐를 얻기 위해 다양한 방법을 채택하였다. 초기의 그래픽카드 구매 열풍에 이어 현재는 여러 명의 사용자가 모여 채굴 그룹을 형성하기도 한다.

이와 함께 주목받는 것이 바로 각 가상화폐의 보상 방식이다. 1300개 이상의 가상화폐는 다양한 보상 방식을 채택하였다. 대표적으로 두 가지의 방법이 있다. 작업증명방식 (Proof-of-Work)과 지분증명방식 (Proof-of-Stake)이다. PoW 방식은 말 그대로 일한 만큼 보상받는 방식이다. PoS 방식은 자신이 원래 보유하고 있던 가상화폐의 지분을 통해 새로운 가상화폐를 배분하는 방식이다.

하지만 이 대표적인 두 증명방식은 단점이 존재한다. PoW 방식은 과다한 전력 사용으로 비경제적이며 채굴을 하기 위해 고성능 하드웨어가 필요하다. PoS 방식은 대량 자금을 가진 사람이 독점하기 쉬우며 신규 참여자가 블록체인 네트워크에 참여하기 꺼려 하는 단점이 있다. 이를 보완하거나 혹은 새로운 개념을 적용시킨 여러 알트코인(Altcoin, 비트코인의 후속작을 통칭하는 용어)이 등장하기 시작했다. 이미 거대해진 비트코인 네트워크에 새로운 기술을 적용하는 것은 매우 힘들기 때문에 현존하는 알트코인들은 자신들의 독자적인 생태계를 구축하는 중이다. 그러나 이 알트코인 또한 기본적으로 PoW, PoS 방식을 완전히 벗어나지는 못하고 있기 때문에 과다한 전력 소모나 독점 문제 등을 해결하기는 어렵다.

따라서 본 논문에서는 PoW, PoS 방식의 단점을 해결하는 방식에 대해 연구하였다. 해당 방식을 본 논문에서는 확률증명방식(Proof-of-Probability)이라 명명하였다. PoP 방식은 각각의 노드가 독자적인 해쉬 정렬 알고리즘(Hash Sorting Algorithm)을 갖는다. 거래 정보

* 1저자, 중앙대학교 분산 플랫폼 및 보안 연구실 (smkim.caucse@gmail.com)
** 2저자, 중앙대학교 분산 플랫폼 및 보안 연구실 (michaela2140@gmail.com)
*** 교신저자, 중앙대학교 분산 플랫폼 및 보안 연구실 (joongheon@cau.ac.kr)

를 블록으로 생성하려 할 때 실제 해쉬 값과 가짜 해쉬 값들을 섞어 블록체인 네트워크에 전송한다. 이때 각 노드들은 자신만의 정렬 알고리즘을 통해 실제 해쉬 값을 찾는다. 실제 해쉬 값을 먼저 찾은 노드가 가상화폐 보상을 받는다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 블록체인에서 가장 유명한 증명방식인 PoW 방식과 PoS 방식에 대해 소개한다. 3장에서는 본 논문에서 제안하는 PoP 방식에 대해 자세히 설명한다. 4장에서는 PoP 방식과 기존 PoW, PoS 방식을 비교 분석한다. 마지막 5장에서는 본 논문을 결론짓고 향후 연구 방향을 제시한다.

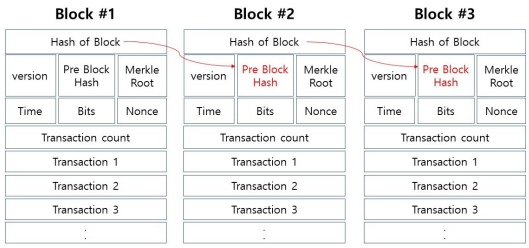
Ⅱ. 관련 연구

2장에서는 블록체인 증명방식 중 가장 대중적인 2개의 합의 알고리즘에 대해 소개한다. 2.1장에서는 PoW 방식에 대해 소개하고 2.2장에서는 PoS 방식에 대해 소개한다.

2.1. PoW (Proof-of-Work)

PoW의 개념은 1993년, Cynthia Dwork 와 Moni Naor에 의해 처음 소개되었다. 그리고 1999년, Markus Jakobsson과 Ari Juels에 의해 Proof-of-Work 라는 이름으로 명명되었다. 이후 2008년, Nakamoto Satoshi가 비트코인 백서에 PoW 방식을 채택하며 PoW는 널리 알려지게 된다[1].

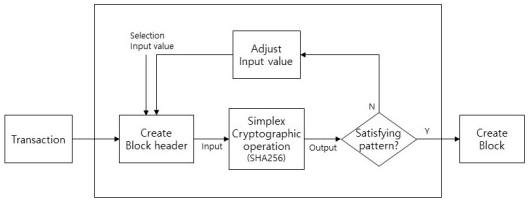
가상화폐로 이루어진 모든 거래(transaction)는 블록체인 안의 블록 속에 저장된다. 이러한 블록의 유효성(Validation)을 검증하는 방식을 Proof-of-Work라 한다. [그림 1]에서 보듯이 블록체인 안의 블록의 구조는 Version, 이전 블록 암호 값(Pre Block Hash), 머클 루트(Merkle Root), 블록 생성 시간, 난이도 설정값(Bits), 난스(Nonce)로 이루어져 있다[2]. 즉 PoW란 난스 값을 찾아내어 거래의 유효성을 증명하는 것이다. 난스 값을 찾아낸 노드(node)는 거래의 유효성을 증명해준 대가로 블록체인의 가상화폐를 받는다. 난스 값을 찾아내는 알고리즘은 [그림 2]와 같다.



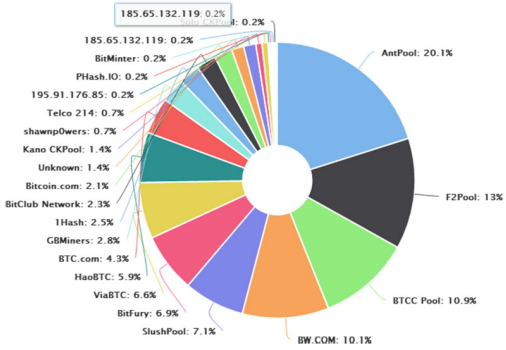
〔그림 1〕 PoW 방식에서의 블록체인 구조

채굴이 가능한 모든 코인은 PoW 방식을 채택하고 있다. PoW 방식을 사용하는 가상화폐가 PoW 방식을 채택한 비트코인에서 출발했기 때문에 가장 대중적이며 시장 규모 또한 PoS 방식에 비해 압도적으로 크다. 이때 채굴을 하기 위해서 채굴자는 입력 값을 하나하나씩 넣어볼 수밖에 없다. 난스 값을 찾기 위해 평균 수천 조 번 이상의 입력 시도가 필요하며 이를 한 사람이 시도하기에는 거의 불가능하다. 이 때문에 마이닝풀(Mining pools)이라는 단체에서 자신들의 컴퓨팅 파워를 할당해주고 해당 단체에서 채굴에 성공했을 시 컴퓨팅 파워를 할당한 양만큼 가상화폐를 나눠 받는 방식이 사용된다[3]. [그림 3]에서 보면 Top4에 해당하는 마이닝풀의 컴퓨팅파워를 합치면 전체 컴퓨팅파워의 50%가 넘는다. 이 마이닝풀들이 연합하여 50% 이상의 컴퓨팅 파워를 가진다면 해당 가상화폐의 보안성은 급격히 악화되는 위험에 처하게 된다.

PoW의 또 다른 단점은 환경적 문제다. PoW 방식은 지속적으로 해쉬를 유지해야 하기 때문에 고성능의



〔그림 2〕 PoW방식에서의 블록 생성 알고리즘



〔그림 3〕 비트코인 마이닝풀의 컴퓨팅파워 지분율

ASIC 및 GPU 구매가 필요하다. 또한 위에서 언급했듯 가상화폐의 채굴을 위해서는 수천 조 번 이상의 입력 시도가 필요한데, 이는 엄청난 양의 전기를 소모한다. PoW 방식을 채택한 대표적 가상화폐인 비트코인과 이더리움(Ethereum)의 전기 소비량은 세계 전기 소비량 72위 국가인 시리아(Syria)보다 높다[4].

이렇듯 PoW의 채굴에 들어가는 많은 비용 및 유지비 (전력 사용, 채굴기 구입 등), 해쉬의 독점으로 인한 보안상의 문제를 해결하고자 2.2에서 설명할 PoS 방식이 나타났다.

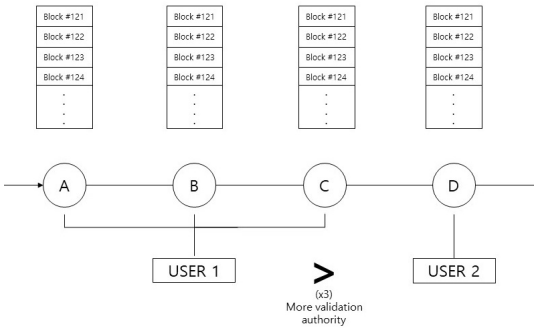
2.2. PoS (Proof-of-Stake)

PoS 방식은 2012년 피어코인(peercoin) 에서 처음 사용되었다. PoW 방식이 컴퓨팅 파워를 통하여 난스 값을 찾고 가상화폐 보상을 받는다면, PoS 방식은 컴퓨팅 파워를 이용하는 채굴이 존재하지 않는다. PoS 방식에서는 [그림 4]에서 볼 수 있듯 자신이 가진 지분(Stake)을 통해 블록 유효성을 검증한다[5]. 이는 주식의 배당금을 지급하는 개념과 비슷하다. PoS 방식의 경우 인터넷이 연결된 PC 1대만 있으면 블록체인 참여가 가능하다. 더 좋은 GPU도 추가적으로 필요하지 않다. 각 가상화폐마다 얻는 방식, 양은 조금씩 다르지만 가지고 있는 가상화폐의 양이 많을수록 더 많은 가상화폐를 지속적으로 얻을 수 있다. 예를 들어 peercoin 100개를 가지고 있는 사람은 peercoin 1개를 가지고 있는 사람에 비해 100배 많은 유효성 검증 자격을 갖게 된다.

PoW 방식의 블록체인에서 새 블록을 생성하는 과정을 채굴이라고 했다면, PoS 방식의 블록체인에서 유효성을 검증하고 새 블록을 생성하는 과정은 포깅(Forging) 이라고 한다. 이때 포거(Forger) 들은 거래 수수료만을 가져간다. 일정한 양 이상의 가상화폐를 가지고 있는 지갑을 블록체인 네트워크에 연결할 때 가상화폐로 보상을 받을 수 있다.

이렇듯 PoS 방식은 PoW 방식 보다 컴퓨팅 파워를 지나치게 사용하지 않아 환경친화적이다. 또한 가상화폐 초기에 대량의 코인이 단기간에 만들어져 점점 줄어드는 PoW 방식과는 다르게 항상 일정한 양이 조금씩 발행되어 Pump and Dump(허위정보를 유포해 가격을 조정하고 차익을 챙겨 빠져나가는 불공정 거래)가 더 적게 일어난다.

하지만 가격 상승 폭이 크지 않다는 특징 때문에 해당 가상화폐 블록체인에 대한 대량 자금 유입이 쉽지 않다. 많은 지분을 가진 사람이 쉽게 독점할 수 있다는 점과 가상화폐를 얻는 이득이 적어 새로운 참여자에게 공정하지 못하는 점이 PoS 방식의 단점이다.



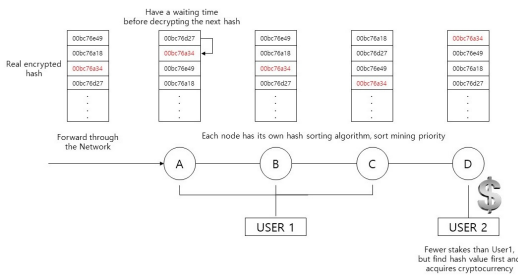
〔그림 4〕 PoS방식에서 지분율에 따른 유효성 검증 자격

Ⅲ. 제시하는 기법

PoW 방식은 지나치게 과열된 채굴로 엄청난 양의 전기를 소모할 뿐 만 아니라 채굴기를 구입하는 비용까지 만만치 않다. 이것을 보완하기 위해 나타난 PoS 방식은 PoW 방식의 경제적인 단점은 해결했지만 새로운 블록체인 참여자가 유입되기 힘든 환경은 만들었고, 많은 지분을 가진 사람이 쉽게 독점할 수 있다. 실제 비트코인 발행지분의 97%를 상위 4%만이 보유하고 있다.[6] 이러한 문제들을 해결하기 위한 기법을 본 논문에서는 PoP(Proof-of-Probability)라 명명하였다.

3.1. PoP 소개

이러한 PoP 방식의 전체적인 구조도는 [그림 5] 과 같다. 각각의 노드(A,B,C,D)는 독자적인 해쉬 정렬 알



〔그림 5〕 PoP 방식의 전체적인 구조도

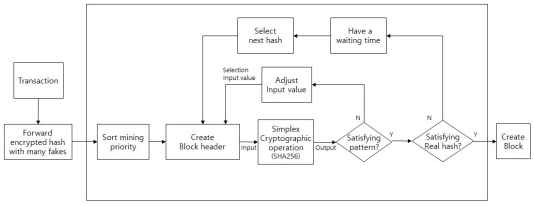
고리즘을 갖는다. 거래가 일어날 시 실제 암호화된 해쉬 값을 포함한 수많은 가짜 해쉬를 네트워크를 통해 전송한다. 각 노드들은 자신만의 해쉬 정렬 알고리즘으로 채굴할 해쉬의 우선순위를 정한다. 정렬된 해쉬에 input 값을 넣어, 계산을 만족한 난스 값을 찾는다. 가짜 해쉬일 경우 대기시간을 가져야만 다음 해쉬의 난스 값을 검증받을 수 있다. 실제 해쉬에 해당하는 난스를 찾은 노드가 해당 블록체인의 가상화폐 1개를 보상받는다.

3.2. 기본 알고리즘

PoP 방식은 위의 [그림 6] 과같이 진행된다.

1) 거래가 발생하면 암호화된 해쉬와 많은 가짜 해쉬를 네트워크상으로 전송한다.
2) 각 노드는 독자적인 해쉬 정렬 알고리즘으로 채굴 우선순위 순으로 정렬한다.
3) 블록 헤더를 생성하고 임의의 난스 값을 대입하여 SHA 단방향 복호화 연산을 한다.
4) 요구 패턴을 만족하지 않았다면 난스 값을 조정하여 3번 과정을 반복한다.
5) 요구 패턴을 만족했다면 해쉬에 해당하는 난스가 진짜 해쉬 값의 난스 인지 검증한다.
6) 진짜 해쉬값이 아니라면 대기시간을 가진 뒤 정렬된 다음 해쉬 값을 선택한 후 3번 과정을 반복한다.
7) 진짜 해쉬 값이라는 것이 증명되면 거래에 대한 블록을 생성한다.

이를 정리하면 [그림 7]의 수도코드와 같다.



〔그림 6〕 PoP 방식의 기본 알고리즘

3.3. PoP 방식의 환경

실제 비트코인에서는 PoW 방식을 채택해 1개의 해쉬를 연산하는데 약 10분의 시간이 걸린다. PoP 방식의

```
if Occur the transaction then
    transmission(hash[])
    newhash[] = sort(hash[])
else
    Wait until create transaction
end if
if GetHash then
    Create transaction block
else
    GetHash
end if
//Definition of each function
procedure SORT(hash[])
    sort hash[] by independent algorithm
end procedure
procedure GETHASH
    while Satisfied with hash[nz] do
        SHA256(nonce)
        gethash = nonce
    end while
end procedure
```

〔그림 7〕 PoP 방식의 수도코드

경우 여러 해쉬를 풀어야 하므로 채굴 난이도(bits) 조절 알고리즘을 이용하여 bits 값을 조절한다[7]. 이때 $5{,}000{,}000\,TH/s$($1\,TH/s$ = 초당 10^{12} 번의 해쉬연산)의 해쉬 파워를 가진 노드 기준, 약 1분의 시간이 걸리도록 조정한다. 이때 x개의 노드가 있을 경우 평균적으로 진짜 해쉬 값을 찾는데 10분의 시간이 걸리도록 하기 위하여 가짜 해쉬를 $10x-1$개만큼 생성한 후 진짜 해쉬를 포함한 $10x$개의 해쉬들을 네트워크 상으로 보낸다. 각 해쉬를 통해 계산한 난스 값을 이진화했을 때 난스의 특정 2^n자리의 bit가 0 일 경우 해당 해쉬는 가짜 해쉬 값이라 구분한다. 난스의 2^n자리의 bit가 1일 경우 해당 해쉬가 실제 해쉬 값이며 블록을 생성한다. 이때 n은 거래가 일어날 때마다 랜덤하게 바뀌며 이 n 값은 유효성 검증자만이 알 수 있다. 또한 계산된 난스가 진짜 해쉬에서 계산된 난스 인지 검증을 받은 후 다음 검증을 받을 때까지 1분의 대기 시간을 두어 해당 노드는 연속적으로 검증을 받을 수 없게 제한한다.

Ⅳ. 분석 및 평가

이 분석 및 평가는 [8]과 유사하게 진행되었다. 4.1장에서는 PoW 방식과 비교하고 4.2.1장에서는 PoS 방식을 분석하고 4.2.2장에서는 본 논문에서 제시하는 PoP 방식을 분석하고 평가한다.

4.1. PoW 방식과의 비교 분석

전체 컴퓨팅 파워 중 채굴자 A가 가지는 비율을 p_A라 가정하자. 이때 채굴자 A가 블록 1개를 채굴할 확률 M_A는 다음과 같다.

$$M_A = \begin{cases} 1 \ , \ p_A \\ 0 \ , \ 1-p_A \end{cases}$$

채굴자 A가 채굴을 하기 위해 하드웨어에 투자한 장비 값을 h_A라 하고 1개의 블록을 채굴하는 동안 사용하는 전기에너지를 E_A라 하자. 1개의 블록을 생성하는 시간 동안의 하드웨어의 가격 변동률은 r이라 한다. 또한 1개의 블록을 생성하는 시간은 일정하다고 가정한다. 이때 n개의 블록을 생성하려고 시도하는 동안 A가 사용한 비용은 $(h_Ar+E_A) \cdot n$ 이다.

블록 1개를 생성했을 때 1개의 가상화폐가 보상되며 이 가격은 K라고 한다. A가 n개의 블록을 얻으려 할 때 A가 얻을 수 있는 비용 C_A는 다음과 같다.

$$C_A = \sum^{n} M_A \cdot K - n \cdot (h_Ar+E_A)$$

M_A는 Bernoulli Distribution을 따르므로 A가 평균적으로 얻을 수 있는 비용 $\mu(C_A)$는 다음과 같다.

$$\mu(C_A) = n \cdot p_A \cdot K - n \cdot (h_Ar+E_A) \qquad (1)$$

현실적으로 채굴자는 블록체인에 참여할 때 금전적인 이익을 봐야지만 노드로 참여한다. 그러므로 채굴자가 얻는 평균적인 비용 $\mu(C_A) > 0$ 를 만족해야 한다.

위의 (1)식을 적용하면 다음과 같은 식을 얻는다.

$$\frac{p_A}{h_Ar+E_A} > \frac{1}{K} \qquad (2)$$

또한 채굴자 A가 처음 블록체인 네트워크에 참여했을 때, 처음으로 가상화폐를 획득하기 전까지 시간이 오래 걸려 채굴자의 예산보다 네트워크 참여비용이 더 소모될 수 있다. 이때 채굴자가 가진 예산을 B_A라 할 때 채굴자가 첫 가상화폐를 획득하기까지 최대한 기다릴 수 있는 시간 T_A는 다음과 같이 정의한다.

$$T_A = \frac{B_A}{h_Ar+E_A} \qquad (3)$$

채굴자는 T_A이전에 가상화폐를 얻어야만 한다. M_A는 Bernoilli Distribution을 따르며 첫 가상화폐를 보상받는데 걸리는 시간 X_A는 다음과 같은 Exponential Distribution으로 나타낼 수 있다. X_A가 T_A보다 클 확률, 즉 A의 예산을 다 쓸 때 까지도 가상화폐를 획득 못할 확률은 다음과 같다.

$$P(X_A > T_A) = e^{-p_AT_A}$$

위의 식에서 T_A가 정의된 (3)식을 대입하면 다음과 같다.

$$P(X_A > T_A) = e^{-\frac{p_AB_A}{h_Ar+E_A}}$$

채굴자가 첫 가상화폐를 늦게 얻어 손해 볼 확률을 α라고 할 때 네트워크에 참여하려면 α보다 작아야 한다. 그때 다음 식을 얻을 수 있다.

$$e^{-\frac{p_AB_A}{h_Ar+E_A}} < \alpha$$

이 식을 정리하면 다음과 같다.

$$\frac{p_A}{h_Ar+E_A} > \frac{-\ln\alpha}{B_A}$$

이 식을 (2)식과 종합하면 다음과 같은 결과를 얻는다.

$$\frac{p_A}{h_A r + E_A} > \max\left[\frac{1}{K}, \frac{\ln\alpha}{B_A}\right]$$

해당 블록체인의 가상화폐 가격 K와 채굴자의 예산 B_A는 상수 값일 때 좌변의 값이 높아질수록 해당 블록체인 네트워크에 쉽게 참여가 가능하다. 이때 PoP 방식은 계산하는 단일 해쉬의 난이도가 PoW 방식의 해쉬 난이도보다 낮으므로 상대적으로 고성능 GPU가 필요하지 않다. 또한 단일 해쉬 연산 속도도 PoW 방식의 비트코인 기준 10분에서 1분으로 감소하여 에너지 소모도 크게 줄었다. 즉 PoW 방식과 비교하였을 때 h_A값과 E_A값이 작아져 같은 가상화폐 가치, 예산이 있을 때 블록체인 네트워크에 쉽게 참여가 가능한 것 뿐 만 아니라 상대적으로 투자 대비 돈을 더 벌수 있는 것을 볼 수 있다.

4.2. PoS 방식과의 비교 분석

4.2.1. PoS 방식 분석

4.1장에서 유사하게 p_B를 전체 블록체인 가상화폐 중 포거 B가 가지는 비율이라 가정하자. PoS 방식에서는 B가 블록 1개에 대한 유효성을 갖고 채굴할 확률 S_B는 다음과 같다,

$$S_B = \begin{cases} 1 \, , \, p_B \\ 0 \, , \, 1 - p_B \end{cases}$$

4.1장과 동일 한 환경조건일 때 B가 얻을 수 있는 비용 C_B와 평균적으로 얻는 비용 $\mu(C_B)$도 마찬가지로 다음과 같다.

$$C_B = \sum^{n} S_B \cdot K - n \cdot (h_B r + E_B)$$
$$\mu(C_B) = n \cdot p_B \cdot K - n \cdot (h_B r + E_B)$$

이때 C_B에 분산을 구하면 Bernoulli Distribution을 따르기 때문에 아래 식과 같다.

$$Var(C_B) = n \cdot p_B \cdot K \cdot (1 - p_B)$$
$$= n \cdot K(p_B - p_B^2)$$

이때 PoS방식에서는 발행 화폐 비율만큼 블록을 생성하기 때문에 계속해서 포깅해도 전체 발행 가상화폐 중 B가 가지는 화폐의 비율 p_B는 수학적 확률로 언제나 일정하다.

4.2.2. PoP 방식 분석

PoP 방식에서 블록체인 네트워크 노드 중 채굴자 C가 가지는 비율을 p_c라 하자. PoP 방식에서 C가 블록을 생성할 확률은 다음과 같다.

$$S_C = \begin{cases} 1 \, , \, p_C \\ 0 \, , \, 1 - p_C \end{cases}$$

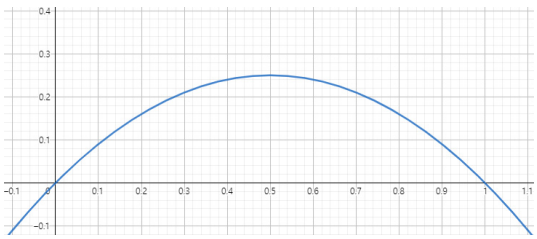
4.2.1장과 동일하게 C가 얻을 수 있는 비용 C_C와 평균적으로 얻는 비용 $\mu(C_C)$도 다음과 같다.

$$C_C = \sum^{n} S_C \cdot K - n \cdot (h_C r + E_C)$$
$$\mu(C_C) = n \cdot p_C \cdot K - n \cdot (h_C r + E_C)$$

이때 C_c에 분산은 아래 식과 같다.

$$Var(C_C) = n \cdot K(p_C - p_C^2)$$

p_C는 0 보다 크고 1보다 작거나 같은 실수로 $(p_C - p_C^2)$를 그래프로 나타내면 [그림 8]과 같다. p_C가 0.5보다 크다는 것은 한 사람이 네트워크 전체 지분 중 절반 이상을 갖고 있다는 것인데 이것은 퍼블릭 블록체인상에서 사실상 불가능하다. 그렇다면 0과 0.5사이에서 해당 그래프는 계속해서 증가한다. 즉 네트워크에서 지분이 증가하면 분산 $Var(C_C)$또한 증가한다. 신규



〔그림 8〕 $y = p_c - p_c^2$ 그래프

참여자 C가 네트워크에 이제 막 참여했을 때 전체 네트워크 상 노드의 지분 p_C는 작을 수밖에 없고 분산 $Var(C_C)$ 도 작을 수밖에 없다. 분산이란 변수의 흩어진 정도를 나타는 지표로 평균값에서 얼마나 벗어나 있는지를 판단하는 값이다. 분산이 작다는 것은 결국 안정적으로 평균값 $\mu(C_C)$에 근접한다는 것이다. 즉 신규 네트워크 참여자는 상대적으로 낮은 위험부담을 갖고 네트워크에 쉽게 참여가 가능하다.

V. 결 론

본 논문에서는 기존 PoW, PoS 방식의 단점을 보완하기 위해 Proof-of-Probability(PoP) 방식을 제안하였다. 단일 해쉬의 난이도가 낮아지고, 한번 해쉬를 검증할때마다 대기시간을 두어 블록체인 네트워크 참여자는 더 이상 높은 하드웨어와 컴퓨팅 파워가 필요하지 않다. 또한 네트워크 참여자가 많을수록 가상화폐의 획득 가능성이 높아지지만 이는 PoS 방식처럼 절대적이지 않으며 신규 네트워크 참여자는 보다 낮은 리스크로 이득을 취할 수 있다. 제안하는 방식은 과열된 하드웨어 성능 열풍을 줄이고 새로운 블록체인 노드 참여를 더 많이 유도할 수 있다는 장점이 존재한다.

참 고 문 헌

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

[2] Shpakovski “Bitcoin Glossary” https://github.com/oleganza/bitcoin-papers/blob/master/BitcoinGlossary.md

[3] Beikverdi, Alireza, and JooSeok Song. “Trend of centralization in Bitcoin's distributed network.” in *Proceedings of the 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2015.

[4] Mark Coppock “The world’s cryptocurrency mining uses more electricity than Iceland” https://www.digitaltrends.com/computing/bitcoin-ethereum-mining-use-significant-electrical-power/

[5] King, Sunny; NADAL, Scott. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” August, 2012, 19.

[6] http://uk.businessinsider.com/bitco in-97-are-held-by-4-of-addresses-2018-1

[7] Bahack, Lear. “Theoretical Bitcoin Attacks with less than Half of the Computational Power” (draft). arXiv preprint arXiv:1312.7013, 2013.

[8] Rosenfeld, Meni. “Analysis of bitcoin pooled mining reward systems” arXiv preprint arXiv:1112.4980, 2011.

[9] S.Kim “POSTER : Mining with Proof-of-Probability in Blockchain” in *Proceedings of the ACM AsiaCCS*, 2018.

〈저 자 소 개〉

김 성 민 (Sungmin Kim)
학생회원

2013년 3월~현재 : 중앙대학교 컴퓨터공학 및 금융공학 학사
관심분야 : 블록체인, 금융공학, Quant

김 경 선 (Kyeong Seon Kim)
학생회원

2017년 8월 : 중앙대학교 컴퓨터공학과 졸업
2017년 9월~현재 : 중앙대학교 소프트웨어공학과 석사과정
관심분야 : 블록체인, 네트워크, IoT

김 중 헌 (Joongheon Kim)
정회원

2004년 2월 : 고려대학교 컴퓨터학과 학사
2006년 2월 : 고려대학교 컴퓨터학과 석사
2006년 3월~2009년 8월 : LG전자 멀티미디어연구소 주임연구원
2014년 8월 : University of Southern California, Computer Science 박사
2013년 9월~2016년 2월 : 인텔 본사 연구원
2016년 3월~현재 : 중앙대학교 소프트웨어학부 조교수
관심분야 : 통신공학, 정보보호