# 검증 가능한 무작위 함수를 사용한 에너지 효율적인 VRF-작업증명 합의 알고리즘

김승민, 최해웅, 이흥노*
광주과학기술원

seungminkim@gm.gist.ac.kr, haeung@gist.ac.kr , *heungno@gist.ac.kr

# Energy-Efficient VRF-Proof-of-Work Consensus Algorithm Using Verifiable Random Function

Seungmin Kim, Haeung Choi, Heung-No Lee*
Gwangju Institute of Science and Technology (GIST)

요 약

작업증명 합의 알고리즘은 블록체인에서 가장 널리 사용되는 합의 알고리즘이지만 많은 에너지를 요구한다. 최근 작업증명의 높은 에너지 소모를 줄이기 위해서 새로운 합의 알고리즘을 개발하는 연구들이 진행되고 있으나, 작업증명에 비해 견고함과 신뢰성이 부족하다. 본 논문은 작업증명에 검증 가능한 무작위 함수(VRF)를 도입하여 에너지 소모를 줄이는 새로운 VRF-작업증명 합의 알고리즘을 제안한다. VRF-작업증명은 VRF에서 일정 값을 얻은 당첨된 노드만 사후 작업증명에 참여할 수 있도록 하여 에너지 소모를 줄인다. VRF-작업증명은 사전 작업증명과, VRF 추첨, 사후 작업증명의 세 단계로 구성되며, 사전 작업증명은 VRF를 당첨될 때까지 무한정으로 실행하는 VRF 반복 공격을 방지한다. 우리는 실험적 분석을 통해 VRF-작업증명이 VRF 반복 공격에 안전하다는 점과 VRF-작업증명이 전통적인 작업증명에 비해서 에너지 효율적임을 입증하였다.

## Ⅰ. 서 론

작업증명(PoW, Proof of Work)은 계산 퍼즐을 해결한 참여자를 의사결정자로 선출하는 합의 알고리즘이다. 작업증명의 보안성은 계산의 난이도에 비례하기 때문에 작업증명 블록체인이 안전하기 위해서는 많은 에너지가 필요하다.[1] 이에 따라 작업증명의 에너지 비효율성을 완화하기 위한 여러 연구가 진행되고 있다.[2]

검증가능한 무작위 함수(VRF)는 타인이 검증할 수 있는 난수 값을 생성하는 알고리즘으로, 블록체인과 같은 분산 시스템에서 중요한 역할을 한다.[3] 작업증명과 VRF를 결합한 접근 방식은 VRF의 무작위성을 통해 일부 노드만 블록 마이닝에 참여하도록 허용하여 에너지를 절약하는 가능성을 제시한다. 본 논문에서는 검증 가능한 무작위 함수(VRF)를 작업증명에 결합하는 새로운 VRF-작업증명 알고리즘을 제안한다. 우리가 제안하는 방식은 사전 작업증명을 실행한 참여자들만이 VRF를 실행할 수 있고, VRF를 통과한 참여자들만 사후 작업증명에 참여할 수 있도록 하는 것이다.

## Ⅱ. 본론

VRF-작업증명은 크게 세 단계로 진행되며, 이는 사전 작업증명, VRF 추첨, 그리고 사후 작업증명의 단계로 구성된다. 첫 번째 단계인 사전 작업증명에서 참여자는 VRF 추첨 단계에 참여할 권한을 획득하기 위해 작업증명을 수행한다. 사전 작업증명은 참여자가 VRF 추첨에 당첨될 때 까지 반복적으로 실행하는 공격을 방지한다. 사전 작업증명을 끝마친 참여자는 VRF 추첨 단계를 실행한다. VRF 추첨 단계는 참여자가 사후 작업증명 단계에 참여할 수 있을지를 확률적으로 결정한다. 이는 동전 던지기 함수와 같이 작동하며, 참여자가 입력으로 사전 작업증명의 결과로 얻은 해시값과 이전 블록의 해시값을 넣으면, 출력으로 사후 작업증명의 참여 가능 여부와 그 증거를 반환한다. VRF 추첨 단계에서 당첨되지 않은 참여자는 블록 생성을 중단하며, VRF 추첨 단계에서 당첨된 참여자는 사후 작업증명 단계를 수행한다. 이 과정은 사전 작업증명과 동일하나 다른 난이도 값과 입력을 가진다. 결과적으로 모든 채굴자 노드가 사전 작업증명을 실행하고, VRF를 통과한 일부 노드들만이 사후 작업증명을 실행하므로, 네트워크의 전체적인 에너지 소모가 절약된다.

VRF-작업증명이 전통적인 작업증명 보다 에너지 효율적이기 위해서는 공격자들의 기대이익 보다 정직한 참여자들의 기대 이익이 더 커야 한다. 공격의 기대 이익이 더 클 경우 모든 노드는 추첨에 당첨될 때 까지 반복적으로 사전 작업증명을 실행할 것이므로 에너지 효율성이 저해된다. 따라서 정직한 참여자의 기대 이익과 공격자의 기대 이익을 비교하여 VRF-작업증명을 검증하고자 한다. 정직한 참여자 $i$가 채굴에 성공할 확률 $p_i$ 는 네트워크의 전체 초당 계산량이 $H$ 이고, 일반 참여자 $i$ 의 초당 계산량이 $h_i$ 라고 할 때, 다음과 같이 계산된다.

$$H = \sum_i h_i$$

$$p_i = \frac{h_i}{H}$$

이 경우, 한 블록의 생성 보상이 $R_{block}$, 사전 작업증명의 난이도가 $D_{pre}$ , 사후 작업증명의 난이도를 $D_{post}$ , $\varepsilon$ 을

난이도 당 비용이라고 할 때, 참여자 $i$의 블록당 평균 보상 $R_i$와 에너지당 이익 $B_i$는 다음과 같다.

$$R_i = p_i * R_{block}$$

$$B_i = R_i - \varepsilon(D_{pre} + pD_{post})$$

공격자의 채굴 방식은 참여자 $i$와 같은 해시 파워를 가지고, $p$의 당첨 확률을 가지는 VRF를 통과할 때까지 사전 작업증명을 반복해서 수행하는 VRF 반복 공격을 시도한다고 가정한다. 공격자는 평균적으로 $p^{-1}$ 번의 사전 작업증명과 한 번의 사후 작업증명을 실행한다. 또한 공격자는 VRF를 통과하여 $p$ 만큼 줄어든 전체 해시파워와 경쟁한다. 이를 반영한 공격자의 확률 $p_a$는 다음과 같으며 공격자의 보상 $R_a$ 와 $B_a$ 는 정직한 참여자와 같은 방법으로 계산된다.

$$p_a = \frac{\frac{h_i}{D_a}}{\frac{p(H-h_i)}{D_{pre}+D_{post}} + \frac{h_i}{D_a}}$$

$$R_a = p_a R_{block}$$

$$B_a = R_a - \varepsilon D_a$$

채산성이 높아질수록, 채굴 비용에 따른 블록 보상이 늘어나므로, 공격 가능성이 커진다. 블록체인의 채산성을 확인할 수 있는 웹페이지인 WhatToMine에 따르면 대부분의 작업증명 블록체인의 채산성은 채굴 비용의 10배 이내이므로, 최악의 상황을 가정해 정직한 참여자의 이득이 소모한 비용의 10배라고 가정한다[4].

$$B_i = 10\varepsilon(D_{pre} + pD_{post})$$

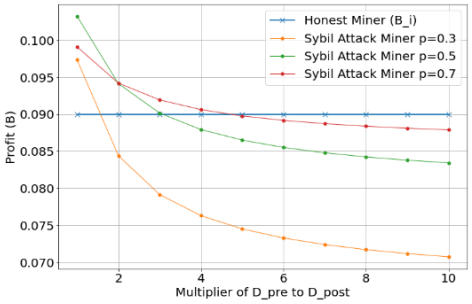


그림 1 $D_{pre}$에 따른 공격자의 이득 $B_a$의 변화

그림 1은 이 가정을 토대로, 블록 보상이 1이고, 공격자의 해시 파워가 전체 해시레이트의 10%일 때, $D_{pre}$이 $D_{post}$의 상수배로 변함에 따라 나타나는 공격자의 이득 $B_a$을 비교 분석한 것이다. VRF 당첨 확률이 증가할 때마다 공격자는 더 적은 횟수를 시도하고 항상 당첨될 수 있기 때문에, 공격자의 이득이 상승하는 결과를 보였으며 $D_{pre}$ 값이 커질수록 공격자의 이득이 감소하는 결과를 보인다. 이 결과를 통해 $D_{pre}$ 를 확률에 따라 충분히 큰 값으로 결정할 경우 VRF-작업증명은 VRF 반복 공격에 안전함을 확인하였다.

작업증명의 블록당 평균 에너지 소모는 블록체인의 난이도에 비례한다. VRF-작업증명과 같은 평균 블록 시간을 가지는 전통적인 작업증명 블록체인을 가정하여 에너지 소모량을 비교하여 VRF-작업증명이 에너지 효율적인지 확인한다. 에너지 소모량은 블록체인의 난이도와 비례하므로, 전통적인 작업증명 대비 VRF-작업증명의 에너지 감소 비율 $E_{vrf}$는 다음과 같다.

$$E_{vrf} = 1 - \frac{D_{pre} + pD_{post}}{D_{pre} + D_{post}}$$

그림 2는 $D_{pre}$이 $D_{post}$의 상수배로 변함에 따라 나타나는 에너지 절감 비율 $E_{vrf}$를 나타낸 것이다.

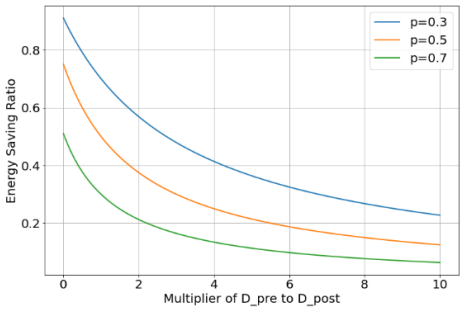


그림 2 $D_{pre}$에 따른 에너지 절감 비율 $E_{vrf}$의 변화

그림 2의 결과는 VRF-작업증명이 전통적인 작업증명 대비 에너지를 효율적으로 절약할 수 있음을 보여준다. $p$가 감소할수록 에너지 감소량이 줄어드는 것을 확인할 수 있으며, $D_{pre}$ 값이 $D_{post}$ 보다 커질수록 모든 노드가 실행해야 하는 작업의 양이 늘어나 에너지 감소량이 줄어드는 것을 확인할 수 있다. 그러나 에너지 소모량을 줄이기 위해 $D_{pre}$ 값이 작고, 높은 $p$ 값을 사용할 경우, VRF 반복 공격에 노출될 수 있으므로 적절한 $D_{pre}$ 값과 확률을 결정해야 한다.

## Ⅳ. 결론

본 논문에서는 검증가능한 무작위 함수를 작업증명 블록체인에 적용한 에너지 효율적인 VRF-작업증명 합의 알고리즘을 제안한다. VRF에 통과한 참여자만이 블록 채굴에 참여할 수 있으며, 사전 작업증명을 도입하여 VRF 반복 문제를 해결하였다. 또한 VRF-작업증명의 에너지 효율성과 VRF 반복 공격에 대해서 분석하여 VRF-작업증명이 에너지 효율적이고 공격에 안전함을 보였다. 추후 연구에서는 네트워크의 컴퓨팅 파워 분포 변화에 따른 VRF-작업증명의 에너지 효율성과 보안성에 대한 분석과 블록체인 확장성에 대한 분석을 진행한다.

## ACKNOWLEDGMENT

This work was supported by the MSIT, Korea, under the ITRC (Information Technology Research Center) support Program (IITP-2024-2021-0-01835) supervised by the IITP (Institute for Information & Communications Technology Planning Evaluation.)

## 참 고 문 헌

[1] Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. Joule, 3(7), 1647-1661.

[2] Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2022). Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. Computer Networks, 214, 109118.

[3] Micali, S., Rabin, M., & Vadhan, S. (1999, 17-19 Oct. 1999). Verifiable random functions. 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039),

[4] WhatToMine. (n.d.). Home Page. Retrieved January 4, 2024, from https://whattomine.com