작업 증명에서 ASIC 저항을 위한 필요조건에 관한 연구

김형성, *이흥노
광주과학기술원

hyoungsung@gist.ac.kr, *heungno@gist.ac.kr

A Study of Requirement for ASIC-Resistant in Proof of Work

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

요 약

작업 증명 알고리즘에서 ASIC 의 등장은 블록 체인의 채굴 참여자의 감소를 유발하여 보안성과 탈중앙화 위협하고 있다. 따라서 작업 증명 알고리즘을 사용하는 블록체인은 ASIC 저항성을 고려해야 한다. 본 논문에서는 ASIC 저항성을 갖추기 위한 필요조건을 두가지 제안한다. 하나는 메모리와 산술 논리 장치의 처리 속도 차이를 이용한 병목 현상 유발이고 다른 하나는 여러 해시 함수를 사용하여 ASIC 등장을 늦추는 설계 난해함이다. 본 논문에서 제안 된 필요 조건을 복합적으로 사용한다면 설계자가 원하는 정도의 ASIC 저항성을 갖춘 작업 증명 블록체인을 설계 할 수 있다.

Ⅰ. 서 론

2008 년 S. Nakamoto 에 의해 작업 증명(Proof of Work)과 해시(Hash) 값을 이용한 블록체인(Blockchain) 이라는 탈중앙화 된 데이터 저장 방식이 제시되었다. [1] 블록체인에서는 참여자들 모두 원장(ledger)을 가지며, 이를 기반으로 후보 블록(Candidate block)을 생성한다. 그리고 참여자들은 합의를 통해 후보 블록 중 하나를 선택 한다. 후보 블록이 선택되지 않은 참여자는 원장을 이용하여 선택된 블록을 검증하고, 블록에 문제가 없으면 과거에 선택된 블록들과 연결하여 블록으로 구성된 체인을 형성한다.

여러 후보 블록 중 하나의 블록이 선택되기 때문에 어떤 블록을 선택 할 것인가에 대한 문제가 존재 한다. S.Nakamoto 는 이 문제의 해결 방법으로 작업 증명이라는 합의 알고리즘을 제시 했다. 작업증명에서는 참여자들은 일련의 해시(Hash) 값들을 무작위로 생성하고 정해진 목표 해시(Target hash)값과 비교한다. 참여자 중 한명이 목표 해시 값보다 작은 해시 값을 발견 했다면 이 참여자의 후보 블록이 선택되어 검증되고, 검증에 문제가 없으면 이전 블록들과 연결 된다. 이 과정은 채굴(Mining)이라고 불리는데, 채굴 과정은 적절한 해시 값을 찾기 위해 매우 많은 연산이 필요하기 때문에 참여자의 후보 블록이 선택 되면, 이 참여자는 채굴 과정의 대가로 보상을 지급받게 된다. S.Nakamoto 는 이 보상의 이름을 비트코인(Bitcoin)으로 명명하였다. 그런데 이 보상의 가치가 매우 높아지면서, 보상을 독점하기 위해 ASIC(Application Specific Integrated Circuit)을 도입하고, 채굴 풀(Mining pool)을 형성하는 집단이 생겨났다..

ASIC 과 채굴 풀의 등장은 작업 증명 블록체인의 보안성과 탈중앙화를 위협하고 있다.

본 논문에서는 ASIC 이 어떻게 보안성과 탈중앙화를 위협하는지 소개 하고, 위협을 회피 하기 위해 ASIC 저항성을 갖기 위한 필요조건들을 제시한다.

Ⅱ. 본론

1. ASIC 의 위협

ASIC 은 CPU 나 GPU 같은 일반 채굴과 비교 했을 때 같은 시간 동안 블록 생성 시도를 더 많이 할 수 있다. 그 결과, 블록을 생성 할 확률이 증가하고 보상을 받을 확률 역시 증가하게 된다. 반대로 CPU, GPU 로 채굴을 하는 참여자들은 보상을 받을 확률이 감소하게 된다. 따라서 ASIC 으로 채굴하지 않은 참여자들의 보상은 점점 감소하게 되고, 채굴에 필요한 비용보다 얻을 수 있는 보상이 적을 때 참여자들을 채굴을 포기한다.

작업 증명에서는 다양한 참여자들이 블록 생성을 위해 많은 시도를 할수록 더욱 강한 보안을 가지게 된다. 따라서 다수의 CPU, GPU 로 채굴하는 참여자가 채굴을 포기하게 된다면 블록 생성 시도 횟수가 감소하고, 결국 ASIC 으로 채굴 하는 사람들에 의해 블록 생성이 독점 된다. 그 결과 블록체인은 탈중앙화를 잃고 ASIC 을 이용한 채굴 참여자들에게 중앙화 되며, 이들은 블록을 위조, 변조 할 수 있는 힘을 가지게 된다. 기존에 생성된 블록이 위조, 변조 된다면 그 블록체인은 더 이상 신뢰 할 수 없는 블록체인이 되기 때문에, 이는 블록체인의 보안에 심각한 위협을 끼치게 된다.

2. ASIC 저항성(ASIC-resistant)

A. 병목 현상 유발(Resistant by Bottleneck)

메모리에서 값을 읽어오는 시간보다 산술 논리 장치(Arithmetic Logic Unit)에서 연산을 처리하는 속도가 더 빠르다면 메모리와 산술 논리 장치사이에서 병목 현상이 발생한다. 즉, 별다른 장치가 없다면, 산술

논리 장치에서 데이터를 처리하는 속도는 메모리에서 값을 읽는 속도에 의존한다. 따라서 채굴 과정에 메모리에서 값을 읽어오는 과정을 추가한다면 채굴기의 성능이 아무리 좋아도 메모리의 입출력 속도에 의해 채굴 속도가 결정된다. 이 방법을 사용한 대표적인 작업 증명은 이더리움(Ethereum)의 Ethash 가 있다[2].

이더리움의 Ethash 작업 증명 방식은 산술 논리 장치의 캐시 메모리에 저장 할 수 없을 정도의 크기의 값을 생성 한 뒤 이 값을 메모리에 저장한다. 채굴을 하기 위해서는 메모리에서 저장된 데이터의 일부분을 선택 한 뒤, 이 데이터를 포함시켜 해시 값을 생성해야 한다. 따라서 ASIC 같은 빠른 처리 속도를 가진 산술 논리 장치라도 앞에서 언급 한 것처럼 메모리의 입출력 속도보다 빠르게 처리 할 수 없다.

B. 설계 난해함(Resistant by Design)

이 방식은 주로 여러 개의 해시 함수를 연속으로 사용하여 ASIC 설계를 난해하게 만든다. 이 방식을 사용한 대표적인 작업 증명 방식은 대시(Dash)의 X11[3]과 레이븐(Raven)의 X16R[4]이 있다. S.Nakamoto 의 작업 증명에서는 해시 값 생성을 위해 SHA-256 한가지만 사용 했던 것과는 달리, 대시의 X11 은 11 가지 종류의 해시 함수를 연속으로 사용하여 ASIC 저항성을 갖추었다. 하지만 2014 년 X11 을 위한 ASIC 이 개발 되었고, 이에 따라 X13, X15, X17 등 해시 함수를 추가 한 알고리즘을 개발하여 ASIC 저항성을 갖기 위한 시도를 계속 하고 있다.

현재 X11 계열에서 가장 진화된 형태는 레이븐의 X16R 이다. 이 방식은 16 개의 해시 값 생성 알고리즘을 이전 블록의 해시 값에 따라 무작위로 변경하여 ASIC 설계를 어렵게 한다. X13, X15, X17 같은 경우 X11 을 바탕으로 설계 했기 때문에, X11 ASIC 을 기반으로 빠르게 ASIC 을 설계 할 수 있다. 하지만 16 개의 해시 함수의 순서가 무작위로 변경되는 X16R 은 ASIC 회로 설계에 고려해야 할 경우의 수가 많아 큰 비용이 필요하고, X11 기반 ASIC 을 사용 할 수 없어 ASIC 등장이 억제 된다는 장점이 있다.

Blake
BMW
Groestl
Jh
Keccak
Skein
Cubehash
Luffa
Shavite
Simd
Echo

Blake
BMW
Groestl
Jh
Keccak
Skein
Luffa
Cubehash
Shavite
Simd
Echo
Hamsi
Fugue
Shabal
Whirlpool
SHA-512

그림 1. (좌) X11 의 해시 함수 (우) X16R 의 해시 함수

Ⅲ. 결론

본논문에서는 작업 증명 방식에 ASIC 저항성을 위한 몇가지 필요 조건을 제안 했다. 더욱 강인한 ASIC 저항성을 가지기 위해서는 여러 특성을 다양하게 조합해서 사용해야 할 필요가 있고, 이를 위한 연구가 계속 되고 있다. [5]

ASIC 을 이용한 채굴은 CPU 나 GPU 를 이용한 채굴과 비교했을 때 압도적인 성능을 가지기 때문에, 채굴 보상을 받을 수 없는 ASIC 을 갖추지 못한 채굴자의 참여를 감소시킨다. 하지만 ASIC 이 구현된 작업 증명 방식의 체인을 공격하기 위해서는 ASIC 의 성능을 크게 상회하는 채굴기를 갖추어야 하기 때문에 CPU, GPU 만 존재하는 작업 증명 방식의 블록체인을 공격 하는 것보다 더욱 큰 비용이 들어 상대적으로 더 좋은 보안성을 갖춘다는 장점이 존재한다. 따라서 작업 증명 방식의 블록체인을 설계하는 사람은 ASIC 의 성능을 어느 정도까지 허용 할 것인가에 대한 고민이 필요하다.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) [NRF-2018R1A2A1A19018665].

참 고 문 헌

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

[2] G.Wood, Ethereum: A Secured Decentralised Generalised Transaction Ledge, 2020, [online] Available: https://ethereum.github.io/yellowpaper/paper.pdf.

[3] Dash document, 2020, [online] Available: https://docs.dash.org/en/stable/introduction/features.html#x11-hash-algorithm.

[4] T.Black, J.Weight, X16R ASIC Resistant by Design, 2020, [online] Available: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf.

[5] RandomX, 2020, [online] Available: https://www.monerooutreach.org/stories/RandomX.php.