# X16R

## ASIC 저항 알고리즘

**트론 블랙, 조엘 라이트**

번역: BPRS by Bradar

(bprs.kr & https://twitter.com/originalbradar)

암호화폐 해싱(데이터를 찾아내는 한 방법)의 역사는 비트코인의 SHA256으로부터 시작하여, 라이트코인의 Scrypt, 이더리움의 Ethash, 대시의 X11를 뒤이어 X13, X15 그리고 X17로 이어졌습니다.

알고리즘 변경의 목적은 특정 코인 채굴의 생태계를 위해 특수제작된 하드웨어의 영향을 최소화하기 위함입니다. 비트코인은 원래 어디에서든 컴퓨터로 채굴될 수 있도록 설계 되었습니다. 비트코인의 가치가 높아짐에 따라, 생산성이 좋은 병렬 처리를 위해 설계된 하드웨어인 그래픽 처리 장치(GPU) 채굴 방식으로 옮겨갔습니다. 채굴의 경제적 가치가 더욱 높아짐에 따라, CPU와 GPU보다 뛰어난, 필드 프로그램 가능 게이트 어레이(FPGA) 형태의 프로그램 하드웨어를 사용하는 것이 가능하게 되었습니다. 다음 단계는 채굴을 위한 특수 제작형 칩을 생산하느 것이였습니다. 주문형 반도체(ASIC)은 경쟁 기술을 지배할 수 있었으며, 효율성의 문제로 다른 어떤 형태(예-GPU,CPU,FPGA)의 채굴을 사실상 불가능하게 하였습니다. 마지막이자, 거의 최종적인 비트코인 채굴의 연산 반복은, 더욱 빠르고 에너지 효율적인 ASIC하드웨어로 옮겨가는 것입니다.

이러한 ASIC 하드웨어로의 전환으로 인한 부작용은 채굴의 중앙 집중화 입니다. 누구나 ASIC을 주문할 수 있지만, 제조 시설 근처에 거주하는 자들에게는 짧은 배송 시간이라는 이점이 있습니다. 또한, 전기 사용량이 채굴의 변동 비용으로 자리잡기에, 저렴한 전기료는 우선 사항입니다. 이로 인해, 몇몇 지역에서 저렴한 비용으로 사용이 가능하며, 대형 ASIC 개발 회사가 있는 중국에서 채굴이 중앙 집중화 되었습니다.

ASIC 채굴의 영향을 최소화 하는 한 가지 해결책은, 메모리 사용 중심의 해싱 알고리즘을 사용하는 것입니다. 이 방식은 라이트코인의 Scrypt와 제트캐쉬의 Equihash를 통해 사용되어 지고 있습니다. 두 가지의 알고리즘은 ASIC의 영향을 줄였습니다. Scrypt를 위한 ASIC 채굴기가 존재하지만, GPU에 비해 상대적인 장점은 작습니다.

또 다른 접근법은 해시 알고리즘의 시퀀스(sequence)를 사용하여, 하나의 출력이 다음 입력으로 이어지게 하는 것입니다. 원래 다크코인 (DarkCoin) 으로 불렸던, 대시(Dash)는 X11 알고리즘으로 이 접근법을 적용 하였습니다. X11은 ASIC 채굴로의 이동을 막기 위해, 11개의 연쇄 해싱 알고리즘을 사용합니다.

이 접근법은 한 동안 문제 없이 진행되었지만, 현재 여러 제조사가 X11용 ASIC 채굴기를 생산하고 있습니다. X11의 기본 개념은 추가 알고리즘으로 확장될 수 있습니다. 이러한 이유로, 일부 코인들은 X13, X15, 심지어는 X17(17개의 연쇄 해싱 알고리즘 사용) 알고리즘을 사용하기도 합니다.

해싱 알고리즘의 고정된 배열은 ASIC 설계에 적합합니다. 더 많은 알고리즘을 결합하면, ASIC을 설계 난이도를 높이지만, X13, X15, 그리고 X17은 모두 X11과 동일한 해싱 알고리즘 배열을 사용합니다. 이것은 추가 해싱 알고리즘을 적용하기 위해서, 기존 설계의 확장만 하면 되기에, ASIC 제조사의 빠른 제조를 가능하게 합니다.

---

[1] https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/

X16R 알고리즘은 해싱 알고리즘의 순서를 지속적으로 방해함으로 인해, 이 문제를 해결하고자 합니다. 해싱 알고리즘은 X15+SHA512에서 사용한 검증된 알고리즘과 동일하지만, 순서는 이전 블록의 해쉬를 기반으로 하여 변경됩니다.

순서의 재배치로 인해 ASIC 설계가 불가능한 것은 아니지만, ASIC이 추가 입력(GPU 또는 CPU 에 의해 더욱 쉽게 달성 가능) 에 적응하는 것을 요구합니다.

X16R 해싱 알고리즘은 이전 블록 해시의 마지막 8바이트(16니블)에 따라 알고리즘의 순서가 바뀌는 블록체인 방식에서 작동하는 16개의 해싱 알고리즘으로 구성됩니다. 이하 전체 알고리즘입니다:

0=blake

1=bmw

2=groestl

3=jh

4=keccak

5=skein

6=luffa

7=cubehash

8=shavite

9=simd

A=echo

B=hamsi

C=fugue

D=shabal

E=whirlpool

F=sha512

**예시:**

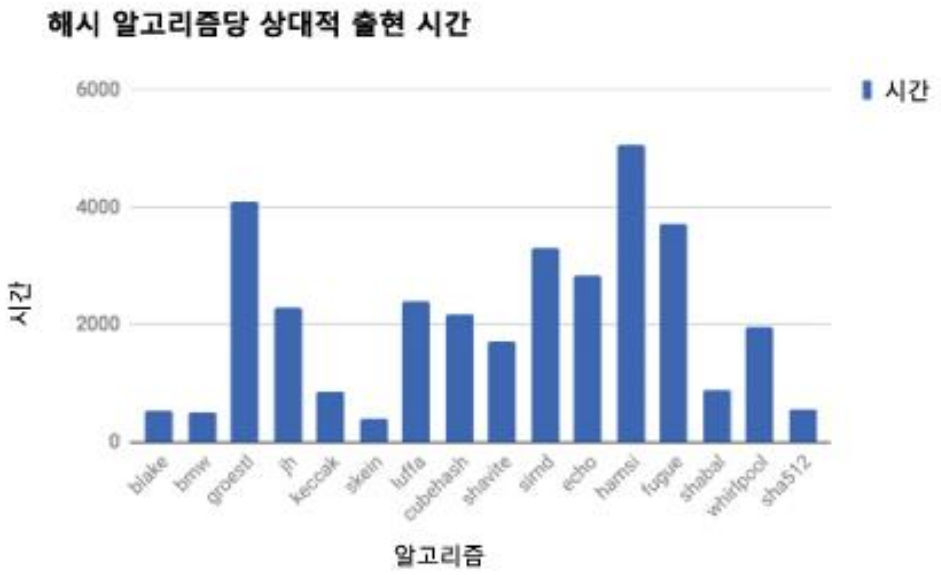
이전 해시 블록:

000000000000000007e8a29f052ac2870045ae3970270f9***7da00919b8e86287***

마지막 8바이트: **0x7da00919b8e86287**

각 16진수(니블)은 다음에 사용될 알고리즘을 결정합니다.

cubehash -> shabal -> echo -> blake -> blake -> simd -> bmw -> simd -> hamsi -> shavite -> whirlpool -> shavite -> luffa -> groestl -> shavite -> cubehash




일부 해시 알고리즘은 다른 알고리즘보다 처리하는 시간이 오래 걸립니다. 이 시간의 차이는 각각의 블록을 채굴하는 동한 16개의 알고리즘에 걸쳐 평균화되는 경향이 있습니다.

이 채굴 알고리즘은 위한 테스트 플랫폼은 '레이븐(RVN)' 입니다. '레이븐'은 비트코인 출시 9주년인, 2018년 1월 3일에 출시 되었습니다. '레이븐'은 비트코인으로 부터 블록당 발행량, 블록타임, 그리고 채굴 알고리즘을 변경 하였습니다.

'레이븐'은 알고리즘의 수량, 사용된 특정한 해싱 알고리즘, 알고리즘의 배열, 그리고 이전 블록 해시로부터 사용된 바이트와 순서를 정의하는 X16R 알고리즘을 위한 참조 구현입니다.

X16R 컨셉의 연장선상에 있는, Scrypt, Equihash, 그리고 다른 ASIC 저항 알고리즘들 또한, 방치된 컴퓨터를 가진 누구든지 기존 규격품(예-GPU) 으로 지속적인 채굴 참여를 가능하게 합니다. 코인의 알고리즘 순서는, 하드웨어 제조사가 X11 알고리즘이 쓰이는 모든 코인(예시)을 위한 ASIC 설계를 어렵게 하기 위해, '쉽게' 변경될 수 있습니다.