해시(Hash)란,해시레이트(Hashrate)란? | 블록체인 용어 소개

원문:
https://www.btcc.com/ko-KR/academy/crypto-basics/what-is-hash-hashrate

이제 막 암호화폐 채굴에 접근한 많은 사람들은 채굴할 때 해시(Hash)나 해시레이트(Hashrate)에 대한 관련 내용을 볼 수 있습니다.

그럼, 해시(Hash) 및 해시레이트(Hashrate)는 무엇입니까? 본문을 보시고 함께 알아보도록 합니다.

해시(Hash)란?

해시(Hash)란, 다양한 데이터를 특정한 함수를 통해 고정된 길이의 출력값으로 변환하는 방법입니다. 데이터의 크기 유형 또는 길이와 관계없이 생성되는 해시는 항상 같은 길이의 출력값을 도출합니다.

블록체인의 암호화폐 , 투표 시스템 등 모든 곳에는 해시가 필수적입니다. 해시는 데이터의 무결성을 위해서 존재합니다. 또한, 블록체인에서 데이터의 무결성이 보장되지 않는다면 사용들의 신뢰 및 사용을 잃게 될 것입니다.

블록 속 데이터가 원본의 상태에서 변형되지 않았다는 것을 증명하기 위해 해시를 사용하여, 데이터가 위조 및 변조되었는지 이를 통해 신뢰 할만한 블록체인인지를 확인할 수 있습니다.

이를 이용해 특정한 배열의 인덱스나 위치나 위치를 입력하고자 하는 데이터의 값을 이용해 저장하거나 찾을 수 있습니다.

기존에 사용했던 자료 구조들은 탐색이나 삽입에 선형시간이 걸리기도 했던것에 비해, 해시를 이용하면 즉시 저장하거나 찾고자 하는 위치를 참조할 수 있으므로 더욱 빠른 속도로 처리할 수 있습니다.

해시(Hash)의 특징

1.고정된 길이의 출력값: 입력됩 데이터의 길이 및 크기에 상관없이 항상 고정된 길이를 출력합니다.

2.무결성:해시는 특정한 데이터를 이를 상징하는 더 짧은 길이의 데이터로 변환하는 행위를 의미합니다. 여기서 상징 데이터는 원래의 데이터가 조금만 달라져도 확연하게 달라지는 특성을 가지고 있어 무결성을 지키는 데에 많은 도움을 줍니다.

예를 들어 'A'라는 문자열의 해시와 'B'라는 문자열의 해시는 고작 한 알파벳이 다를뿐이지만 해시 결과값은 완전히 다른 문자열이 나오게 됩니다.

3.충돌 회피성:해시의 출력값이 출돌할 가능성은 희박합니다. 해시가 서로다른 두개의 입력값에 대해 동일한 출력값은 도출하는 상황을 의미합니다. 이록적으로 입력을 무한대로 할 수 있다면 충돌을 찾을 수 있으나, 현 지구상의 모든 컴퓨터를 동원해도 불가능합니다.

4.단방향성:해시는 블록 속 데이터를 한 방향으로만 변환하며, 역산은 불가능합니다. 그렇기 때문에 출력값만으로 입력값을 차을 수 없습니다.

덧붙여,해커들의 역산을 통한 해킹은 사실상 불가능합니다. 이와의 Brute-Force(무적위 대입) 공격만이 유일한 방법이지만 해시 알고리증과 암호화 알고리증을 추가하거나, 솔트값(Salt:소금이라고 불리는 임의의 값을 해시하기 전에 붙여 해시 값을 무작위로 만듦)을 추가하여 이 점을 보완합니다.

5.임의성:해시는 출력값을 도출하는 공식을 찾을 수 없게 일정한 포맷을 기준으로 임의로 출력값을 변환합니다.

해시(Hash)의용도

해시는 블록체인과 IPFS 등 다양한 분야에서 활용되고 있습니다. 보안 분야에서도 널리 사용되는데 이는 해시 함수가 원래의 문장을 복호화할 수 없게 뭉개버린다는 장점과 원문과 해시값 사이에 선형적 관계가 없다는 특성을 지니고 있기 때문입니다.

해시 함수의 결과물은 고정된 길이의 숫자이므로, 원래의 정보는 손실되는데, 이러한 특성 때문에 하나의 원 데이터는 하나의 해시값만 가지지만, 하나의 해시값을 만들어 낼 수 있는 원본 데이터는 매우 많아서, 해시값만 가지고는 아무리 용을 써도 이미 뭉개져버린 원문을 복원해해는 것은 불가능합니다.

따라서 비밀번호, 전자서명, 전자투표, 전자상거래와 같은 민감한 입력의 무결성을 검증할 때 주로 사용됩니다.

데이터의 무결성과 직접적인 연관이 있기 때문에 어떤 해시 함수에서 해시 충돌이 일어나기 쉽다는 것은 보안 분야에서는 매우 민감한 문제에 해당합니다.

해시레이트(Hashrate)란?

해시레이트(Hashrate)란 연산 처리능력을 측정하는 단위로 해시 속도를 의미합니다. 작업증명(PoW) 합의 알고리즘을 사용하는 모든 암호화폐에서 나타납니다.

해시레이트가 높다는 말은 연산 처리 능력이 높아져 더 빠른 채굴이 이뤄진다는 것, 곧 채굴 난이도가 상승하는 걸 의미합니다. 일반적으로 해시레이트가 높아져 연산량이 많아질 경우, 더 빠른 채굴이 이루어지기 때문에 채굴 난이도가 높아집니다.

채굴 난이도가 높아지면 시중에 비트코인 공급량이 줄어들어 이는 흔히 장기 가격 상승을 예측하는 지표로 활용되기도 합니다.

해시레이트란 초당 해시값 계산 횟수의 총합으로 암호화폐의 연산 작용 과정에서 얻을 수 있는 채굴의 성공 확률과 실제로 채굴에 성공한 시간으로부터 도출되는 이론값이라고 할 수 있습니다.

간단히 말하면 해시레이트는 주어진 채굴기가 작동하는 속도로 정의 내릴수 있다. 암호화폐 채굴에는 복잡한 계산을 통해 블록을 찾는 것이 포함된다. 블록은 수학 퍼즐과 같아서 채굴기는 블록을 해결하기 위한 올바른 답을 찾기 위해 초당 수천 또는 수백만 건의 추측을 해야 합니다.

해시레이트는 채굴로부터 얼마나 많은 수익을 얻을 수 있는지에 큰 영향을 미칩니다. 점 더 많은 비트코인이 채굴되면서 해결해야 할 방정식이 점점 더 복잡해졌고, 복잡성이 증가함에 따라 채굴작업은 경쟁력을 갖추기 위해 해시레이트를 높혀야 합니다.

해시레이트 계산방법은?

현재 정확한 비트코인 해시레이트를 산출할 수 없습니며 추정치만 할 뿐입니다. 해시율은 전통적으로 비트코인의 공개 데이터를 기반으로 추정됩니다.

이런 전통적인 추정방법은 정확했지만, 이런 방법은 오랫동안 부정확하다는 비판을 받아왔습니다.

암호화폐 거래소 크라켄(Kraken)은 통계를 사용하여 해시율이 95% 신뢰도로 특정 범위 내에 있음을 보여주는 또 다른 방법을 제시했습니다.

해시레이트 왜 중요합니까?

해시율은 블록체인 네트워크의 강도와 보안을 반영하는 중요한 지표입니다. 채굴자가 다음 블록을 발견하는 데 사용하는 머신이 많을수록 해시율이 높을수록 악의적인 에이전트가 네트워크를 방해하기가 더 어려워집니다.

예를 들어 51% 공격은 단일 개인 또는 공격자 그룹이 블록체인 해시레이트의 50% 이상을 제어할 수 있는 충분한 채굴 장비를 구매하거나 임대하는 경우입니다.

블록체인은 신뢰할 수 없고 "가장 긴 체인 규칙"란 것을 따르기 때문에 해시 비율의 대부분을 제어하는 개인이나 그룹은 이론적으로 거래를 차단 또는 재구성하거나 자체 지불을 취소할 수도 있습니다. 이것은 기본 블록체인의 무결성을 완전히 파괴하는 이중 지불 문제를 일으킬 것입니다.

따라서 해시레이트가 떨어진다는 것은 51% 공격을 수행하는 데 드는 비용이 낮아져 네트워크가 공격에 더 취약하다는 것을 의미합니다.