BlockChain

2018년 11월 24일 토요일 오전 12:53

시작하기 전에 블록체인과 비트코인의 구분 정도는 해보자. 블록체인은 비트코인의 운영 바탕이 되는 체계이고, 비트코인은 블록체인을 화폐 발행과 운영에 응용한 것이다. 고로 핵심이 되는 기반 기술 체계는 블록체인이고, 비트코인은 블록체인을 바탕으로 만들어낸 서비스의 하나이다.
그럼 블록체인이 어떻게 작동하는지 기초부터 한 번 들여다보자.

BlockChain

블록체인은 최초의 블록(Genesis Block)부터 시작해서 바로 앞의 블록에 대한 링크를 가지고 있는 링크드 리스트다. 블록체인은 여러 노드에 걸쳐 분산되어 저장 및 관리되며, 블록에는 거래 정보가 포함되어 있으므로, 블록의 집합체인 **블록체인은 모든 거래 정보를 포함하는 거대한 분산 장부**라고 할 수 있다.

Block

블록은 블록체인의 원소로서 개념적으로는 **다수의 거래 정보의 묶음**을 의미한다.
블록은 블록 헤더와 거래 정보, 기타 정보로 구성된다.

- 블록 헤더는 version, previousblockhash, merklehash, time, bits, nonce 이렇게 6개의 정보로 구성된다.
- 거래 정보는 입출금과 관련한 여러가지 정보를 가지고 있다.
- 기타 정보는 블록 내에 있는 정보 중에서 블록 헤더와 거래 정보에 해당하지 않는 정보를 말하며, 블록 해쉬 계산에 사용되지 않는다.

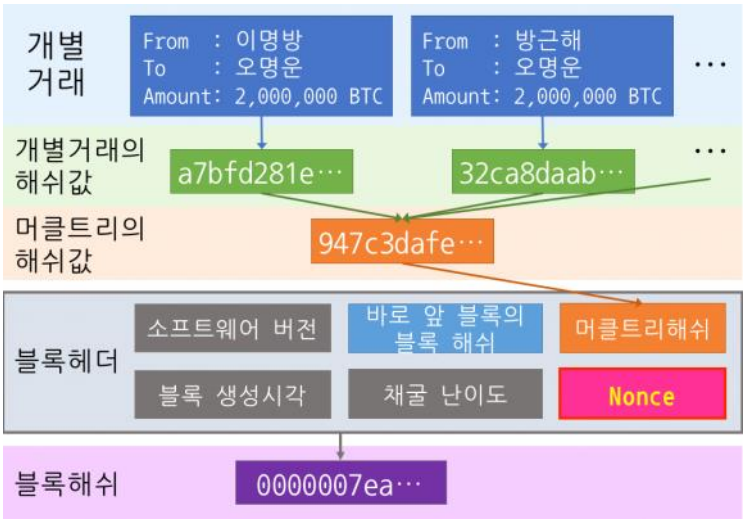
Block Header

블록 헤더는 다음의 6가지 정보로 구성

1. version : 소프트웨어/프로토콜 버전
2. previousblockhash : 블록 체인에서 바로 앞에 위치하는 블록의 블록 해쉬
3. merklehash : 개별 거래 정보의 거래 해쉬를 2진 트리 형태로 구성할 때, 트리 루트에 위치하는 해쉬값
4. time : 블록이 생성된 시간
5. bits : 난이도 조절용 수치
6. nonce : 최초 0에서 시작하여 조건을 만족하는 해쉬값을 찾아낼때까지의 1씩 증가하는 계산 회수

Block Hash

블록의 식별자 역할을 하는 블록 해쉬는 6가지의 블록 헤더 정보를 입력값으로 하고, 여기에 SHA256 해쉬 함수를 2회 적용해서 계산되는 값으로, 32바이트의 숫자값이다. **이름은 블록 해쉬이지만 그 값은 블록 전체를 해쉬한 값이 아니라, 블록 헤더를 해쉬한 값**이다.
지금까지의 내용을 바탕으로 블록 해쉬를 구하는 과정을 그림으로 나타내면 다음과 같다.



이제 이 그림을 중심으로 얘기를 풀어가보자.

완료된 거래 정보의 변경이 사실상 불가능한 이유

거래 정보의 해쉬값은 해당 거래가 포함된 블록의 merklehash 계산에 입력값으로 사용되고, merklehash는 블록 해쉬의 계산에 입력값으로 사용된다. 블록 해쉬는 다음 블록(A라 하면)의 previousblockhash 값으로 저장되며, previousblockhash은 A 블록의 블록 헤더 정보로서, A 블록의 블록 해쉬를 계산하는데 입력값으로 사용된다.

따라서, 거래 정보가 변경되면 merklehash가 변경되고, merklehash가 변경되면 블록 해쉬가 변경되고, 블록 해쉬의 변경은 다음 블록의 블록 해쉬 변경으로 연쇄적으로 이어지게 된다. 그리고 블록 해쉬는 작업 증명의 해답(nonce값)을 찾아내야 구할 수 있으므로, 거래 정보를 변경한 블록부터 그 이후의 모든 블록을 순서대로 다시 채굴해야 한다.

블록 하나 채굴하는데 평균 10분이 소요되고, http://bitcoincharts.com/bitcoin/ 에서 확인한 2016-01-23 현재 총 블록 수가 약 40만 블록이므로, 최초의 원조 블록인 Genesis 블록에 포함된 거래를 변경하면 약 400만 분, 약 7.6년의 시간이 소요된다.

그 7.6년의 시간 동안에도 새로운 블록들도 평균 10분 마다 하나 씩 계속 생성되므로 이를 모두 뒤집는 것은 사실 상 불가능하다.

완료된 거래 정보를 변경하려면,

변경하려는 거래 정보가 포함된 블록부터 그 이후의 모든 블록을 순서대로 다시 채굴해야 하는데,

이는 많은 시간이 소요되고, 그 동안 다른 노드들에 의해 블록이 계속 추가되므로, 완료된 거래 정보의 변경은 현실적으로 사실상 불가능하다.

채굴

채굴은 일반인들이 비트코인을 쉽게 이해할 수 있도록 만든 용어로서, **작업 증명(Proof of Work)과 보상을 합친 개념**이라고 생각하면 된다.

Proof of Work(작업 증명)

작업 증명은 새로운 블록을 블록체인에 추가하는 '작업'을 완료했음을 '증명'하는 것이라고 이해하면 된다. 새로운 블록을 블록체인에 추가하려면, 그 새로운 블록의 블록 해쉬를 계산해내야하고, 그 블록 해쉬를 계산해내려면 그 블록의 블록 헤더 정보 중의 하나인 nonce값을 계산을 통해 구해야 한다.

결론적으로 이 nonce값을 구하는 것이 바로 작업 증명이다.

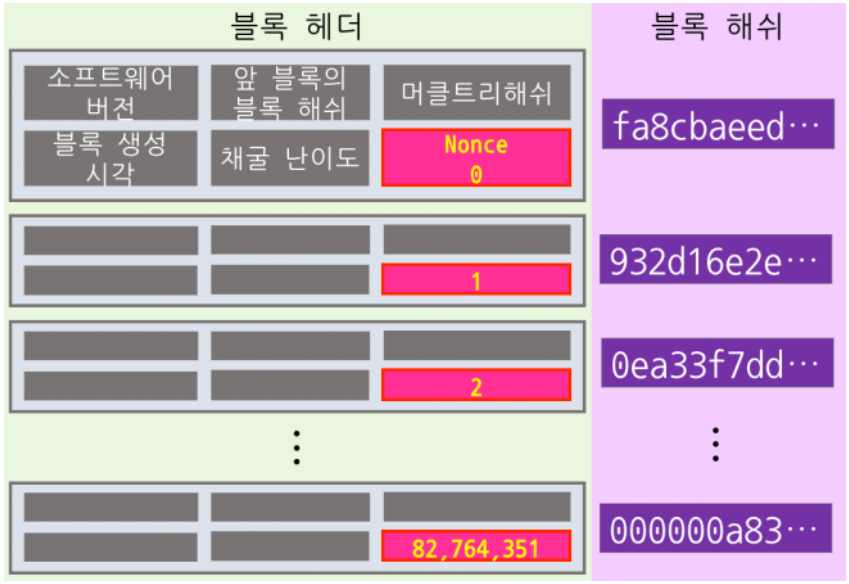
nonce 값의 계산

결론부터 말하면 nonce 값은, 이 nonce 값을 입력값 중의 하나로 해서 계산되는 **블록 해쉬값이 특정 숫자보다 작아지게 하는 값**을 말한다.

그리고 해쉬 함수의 특성상, 어떤 해쉬값(A라고 하면)을 결과로 나오게 하는 입력값을 찾으려면, A에서 역산을 하는 방식으로는 찾을 수 없고, 결과가 A가 될 때까지 무작위로 입력값을 계속 바꿔가면서 찾아낼 수 밖에 없다.

그 입력값을 바꿀 수 있는 유일한 통로가 바로 nonce다. 다시 말해, 아래 그림의 '블록 헤더'란에 포함된 6가지 정보 중에서 확정되지 않아서 값을 바꿀 수 있는 유일한 항목이 nonce다.

이 nonce 값을 1씩 증가시키면서 반복적으로 계산한 블록 해쉬값이 특정 숫자보다 작은 값이 나오면, 그 때의 nonce 값으로 계산한 블록 해쉬가 그 블록의 블록 해쉬로 확정되고, 블록 해쉬라는 식별자를 얻은 그 블록은 새로운 블록으로서 블록 체인에 추가되며 작업이 완료 된다.
블록 해쉬가 특정 숫자보다 낮게 나올 때의 nonce 값이 바로 작업 증명을 나타내는 nonce 값이다.
이 과정을 그림으로 살펴보면 아래와 같다. 아래의 그림은 블록 해쉬가 000000a84...보다 작게 나오는 nonce값을 구하는 과정을 나타내고 있다.



앞에서 설명한 대로 nonce 외의 모든 항목의 값은 이미 정해져 있다.
nonce 값이 0 일 때의 해쉬를 구해보니 000000a84...보다 큰 fa8cbaeed... 가 나와서 작업 증명에 실패 했다.
다시 nonce가 1 일 때의 해쉬를 구해보니 932d16e2e... 가 나와서 또 실패.. nonce가 2 일 때의 해쉬, 3 일 때의 해쉬.. 를 계속 반복해서 구하고 실패하다가, nonce가 82,764,351 일 때의 해쉬를 구해보니 드디어 000000a84...보다 작은 000000a83...이 나와서 작업 증명에 성공했다.
그렇다면 작업 증명 성공 여부의 기준이 되는 000000a84...라는 값은 어떻게 정해지나?
바로 **작업 난이도**에 의해 정해진다(앞의 그림에서는 이해를 돕기 위해 작업 난이도보다는 더 구체적인 채굴 난이도로 표시했으나, 이제 그 작업이 무엇인지 알았으니 앞으로는 작업 난이도라고 한다.)

작업 난이도

블록 해쉬가 특정 숫자보다 낮게 나올 때의 nonce 값을 찾아내는 것이 작업 증명이라고 했다. **작업 난이도는 nonce값 계산의 어려운 정도**를 나타낸다. 작업 난이도는 블록 헤더 정보에서 bits라는 값으로 조절된다.

앞에서 블록 해쉬는 32바이트의 숫자라고 했는데, 이해를 쉽게 하기 위해 블록 해쉬를 부호 없는 1바이트의 숫자라고 해보자. 그럼 1바이트의 숫자값을 블록 해쉬값으로 산출하는 해쉬 함수는 0 ~ 255 사이의 값을 결과로 산출한다.
블록 해쉬가 128보다 작아야 한다고 하면, 0 ~ 255 사이의 값을 산출하는 해쉬 함수를 적용해서 128보다 작은 블록 해쉬값이 나올 확률은 128보다 작은 수(0~127)의 개수 = 128/해쉬 함수가 산출할 수 있는 모든 값(0~255)의 개수 = 256, 즉, 128/256이므로, 50%의 확률이다.
블록 해쉬가 64보다 작아야 한다면 64/256, 즉 25%의 확률로 nonce 값을 구할 수 있다. 블록 해쉬가 32보다 작아야 한다면 확률은 12.5%로 줄어든다. 여기서 128, 64, 32라는 특정 숫자가 바로 블록 헤더 정보의 bits이다.
실제로 bits의 값이 128, 256 이런 식으로 저장되지는 않고, 지수와 계수를 사용하는 별도의 표현 방식이 있다.
난이도는 2,160개의 블록이 생성되는데 소요되는 시간이 평균 시간인 21,600분(10분/블록 * 2,160블록)보다 오래 걸리면 낮아지고, 적게 걸리면 높아지는 방식으로, 대략 21,600분을 주기로 전체적으로 평균 10분이 소요되는 하나의 난이도가 전체에 적용된다.
블록 헤더의 bits는 nonce 값을 계산하는데 기준이 되는 특정 숫자를 나타내며,
블록체인 전체에 걸쳐 일률적으로 적용되는 숫자다.

보상

보상은 **새로 발행되는 비트코인과 해당 블록에 포함되는 거래의 거래 수수료의 합**이다. 비트코인의 새로운 발행은, 채굴자가 블록을 처음 구성할 때 채굴자의 지갑으로 일정량의 비트코인이 입금되는 거래를 그 블록의 첫 거래(generation transaction)로 추가하는 방식으로 이루어진다. 새로 발행되는 비트코인은 최초에 50BTC에서 시작해서 블록 체인에 21만개의 블록이 추가될 때마다 절반으로 줄어든다.
거래 수수료는 각 거래 당사자끼리 자율적으로 정할 수 있고, 거래가 블록에 추가되는 우선 순위를 결정하는데 거래 수수료가 입력값으로 사용되기도 한다.
보상은 nonce 값을 찾아내고, 그 결과 새로운 블록을 블록 체인에 추가해서,
해당 블록에 포함된 모든 거래를 유효한 거래로 확정시켜준 대가라고 할 수 있다.

채굴 보상이 줄어든다면 채굴에 의해 유지되는 블록체인이 지속될 수 있나?

비트코인의 총 발행량은 2,100만BTC로 정해져 있다. 결국 채굴하더라도 언젠가는 비트코인은 더 이상 발행되지 않으므로, 거래 수수료만이 유일한 보상으로 남게 된다.
어떤 상황에서든 채굴이 의미가 있으려면, 채굴에 소요되는 비용보다 수익이 더 커야하며, 이는 비트코인의 신규 발행이 없는 상황에서도 마찬가지다. 이 조건을 만족시켜야 채굴이 계속되고 블록체인이 지속될 수 있다. 비트코인 신규 발행이 없는 상황에서 이 조건이 만족되려면 다음과 같은 시나리오가 충족되어야 한다.

채굴 비용의 감소

채굴 비용의 감소는 결국 작업 증명 해답을 찾는데 얼마의 시간이 소요되느냐에 달려있다. 이는 작업의 난이도에 달려 있으므로, 거래 수수료만이 유일한 보상인 상황에서 블록체인이 유지되려면 작업의 난이도가 현재보다 더 낮아져서 소요 비용을 낮춰야 할 것이다.

거래 수수료의 증가

거래 수수료의 증가는 결국 거래 수수료율의 증가를 의미하는데, 거래의 성격과 다른 화폐와의 경쟁 등 시장 상황에 따라 정해지겠으나 대폭 높아지기는 어려울 것이다. 따라서 수수료율의 증가가 아니라 수수료 총액의 증가로 이어질 것이다. 즉, 블록의 크기를 늘려서 블록 안에 더 많은 거래를 담아서 블록 당 수수료 총액을 높게 유지하는 방식으로 전개될 것이다.
신규 발행이 사라지는 2140년 경 이후에는 결국은 채굴 난이도가 낮아지거나 블록 크기를 늘리는 방식으로 블록체인이 유지될 것이다.

정리

- 블록체인은 모든 거래 정보를 포함하는 거대한 장부로서, 여러 채굴자의 컴퓨터에 복제되어 관리되는 분산 장부다.
- 블록은 다수의 거래 정보의 묶음이며, 이런 블록이 체인처럼 연결되어 전체 블록체인을 형성한다.

- 채굴은 블록에 담긴 거래 정보를 유효한 것으로 확정시키기 위해 어떤 숫자값을 찾아내는 작업 증명(Proof of Work)과 그에 따른 보상을 합친 개념이다.
- 비트코인은 블록체인 시스템을 암호화 화폐 분야에 적용한 서비스의 일종이다.

출처 : https://homoefficio.github.io/2016/01/23/BlockChain-%EA%B8%B0%EC%B4%88-%EA%B0%9C%EB%85%90/