Bithumb Economic Research Institute

2022.08.12

Bithumb's Guest Opinion

비트코인 채굴자들은 무엇을 하는걸까?

Bithumb's Guest
백훈종 샌드뱅크 COO

bithumb

비트코인 채굴자들은 무엇을 하는걸까?

비트코인 채굴은 많은 오해를 받는 산업이다. 컴퓨터 코딩이나 암호학에 익숙지 않은 일반 투자자들은 실제 금광에서 광부들이 금을 캐내듯, 채굴자가 컴퓨터 어딘가에서 비트코인을 찾아 끄집어낸다고 생각하기도 한다. 그 말이 전부 틀린 말은 아니지만, 컴퓨터가 비트코인을 채굴하는 과정은 금광에서 광부가 곡괭이를 휘두르는 과정과는 사뭇 다르다.

입문자들은 도대체 왜 '채굴 (Mining)'이라는 표현을 쓰는 것인지부터 헷갈릴 것이다. 데이터 센터같이 생긴 큰 공장에 수많은 기계가 꽉꽉 들어차 있고, 윙윙거리는 소리를 내며 가동되고 있을 뿐인데 대관절 무엇을 어떻게 채굴한다는 것일까? 채굴자들은 비트코인 네트워크가 내는 복잡한 문제를 빨리 풀어야 보상받는다는데, 대체 얼마나 복잡한 문제길래 컴퓨터 기기가 저렇게 많이 필요한 것일까?

채굴은 문제를 먼저 풀어 블록 생성 권한을 얻는 과정

채굴은 비트코인 네트워크가 내는 문제를 남들보다 먼저 풀어 다음 블록을 생성할 수 있는 권한을 얻는 과정이다. 블록을 생성한 채굴자에게는 채굴 보상(블록당 6.25BTC)과 전송수수료(그때그때 다름)가 주어진다.

비트코인 채굴자들이 수많은 컴퓨터를 채굴에 동원하는 이유는 이 문제를 남들보다 더 빨리 풀어 이 보상을 획득하기 위함이다.

그런데 알고 보면 이들이 수행하고 있는 작업이 그렇게 복잡한 일이 아니다. 어떤 과정으로 이루어지는지만 정확하게 이해하면 컴퓨터가 없어도 비트코인을 채굴할 수 있을 정도다. 사실 펜과 종이만 있어도 비트코인 채굴 경쟁에 뛰어들 수 있다. 물론 당신의 계산 속도가 컴퓨터보다 빠르다는 전제하에 말이다.

비트코인 네트워크의 SHA-256 알고리즘

비트코인 네트워크는 채굴자들에게 문제를 내기 위해 SHA-256이라는 것을 사용한다. SHA-256의 사전적 정의는 "SHA(Secure Hash Algorithm) 알고리즘의 한 종류로서 1993년 미국의 국립표준 기술연구소에 의해 공표된 표준 해시 알고리즘인 SHA-2 계열 중 하나이다..." 라고 하는데, 설명이 너무 복잡하므로 일단 신경 쓰지 않아도 된다.

SHA-256은 간단히 말해서 어떤 메시지이든 256비트(bits)의 2진수 메시지로 전환하는 기능을 말한다. 아무 메시지나 SHA-256에 입력하면 SHA-256은 그것을 뭔가 다른 형태로 변환하여 결과값으로 내뱉는다. SHA-256이 이렇게 원래 메시지를 다른 형태로 변형하여 내뱉는 결과값을 바로 '해시(Hash)'라고 한다.

SHA-256에 입력하는 메시지의 길이는 아무리 길어도 상관없다. 무슨 입력값을 입력하든 SHA-256은 반드시 256개의 '0'과 '1'로만 이루어진 메시지를 내뱉는다. 예를 들어, '샌드뱅크'라는 단어를 SHA-256에 입력하면 다음과 같은 결과값이 나온다.

```
0010001001001011110111000000100000000001000011100101001110101011011111100011000010110001101101010110010011101010111011101001111100000001011101111011100111111101110011011110101111101100101011101011011010100100111011011010000101001010001101111101000000000
```

보다시피 총 256개의 '0'과 '1'로 이루어진 메시지 (또는 '해시')가 탄생했다. '샌드뱅크'라는 메시지를 입력하면 SHA-256은 항상 똑같은 값을 내놓을 것이다. 그러나 만약 입력값을 '샌드뱅크'에서 살짝만 바꾼 '샌드뱅쿠', '샌드뱅코' 등으로 입력하면 완전히 다른 결과값이 나온다.

아무리 긴 메시지라도 SHA-256에 집어넣고 256개의 '0'과 '1' 형태로 바꿀 수 있지만, 그렇게 나온 결과값으로 다시 원래 메시지를 유추하는 것은 불가능하다. 한마디로 SHA-256을 통한 메시지 변형은 '편도'이지 왕복이 아니다.

무한에 가까운 경우의 수 가운데 답을 찾는 과정

여기서부터가 중요하다. 위의 예시를 보면 맨 앞에 '0'이 두 번 연속으로 나온 것을 알 수 있다. SHA-256은 어떤 메시지이든 '0'과 '1'로만 변환하므로 맨 앞자리 숫자에 '0'이 나올 확률은 50%이다 ('0' 아니면 '1'이므로).

그 다음에도 '0'이 또 나올 확률은 25% (50% x 50%), 세 번 연속으로 '0'이 나올 확률은 12.5% (50% x 50% x 50%)로 확률은 갈수록 줄어든다. 비트코인 네트워크는 채굴자들 간의 경쟁이 얼마나 심한지를 판단하여 2주에 한 번씩 채굴 난이도를 조절하는데, 현재 난이도 기준으로 채굴자들은 맨 앞에 19개의 '0'이 연속으로 나오는 '해시'를 결과값으로 얻어야 한다.

어떤 메시지를 SHA-256에 입력해야 19개의 0이 연속으로 나올 것인가. 바로 이 입력값을 맞추는 것이 채굴자들이 해야 할 일이다. 게다가 비트코인은 'Double SHA-256'이라고 불리는 방법으로 가뜩이나 어려운 문제를 더 어렵게 한 번 더 꼬았다. 'Double SHA-256'은 간단히 말해서 어떤 입력값을 SHA-256에 입력하여 결과값을 얻고, 그걸 다시 SHA-256에 입력하여 두 번째 결과값을 얻는 방식이다. 동전 던지기와 비교하면 무작정 동전을 던져서 19번 연속 앞면이 나오게 하는것이 아니라, 동전 두 개를 동시에 던져 둘 다 앞면이 19번 연속 나오게 하는 것과 비슷하다.

채굴자들이 찾아야 하는 입력값의 앞부분은 해당 블록에 담길 데이터이다. 그 뒤에 어떤 숫자나 문자가 오느냐에 따라 SHA-256이 뱉어낼 결과값은 천차만별로 달라진다. 결국 채굴자들은 이 알 수 없는 미지의 숫자, 또는 문자를 찾아내기 위해 거의 무한대에 가까운 경우의 수와 싸워야 한다. 여기서 채굴자들이 찾아내야 하는 미지의 숫자, 또는 문자를 바로 '논스(Nonce)' 라고 한다.

SHA-256 연산으로 직접 논스를 찾아보자

이제 비트코인 채굴자들이 왜 엄청난 규모의 채굴시설을 운영해야 하는지 이해할 수 있을 것이다. 거의 무한대에 가까운 경우의 수를 극복하기 위해서는 대규모 연산력이 필요하다. 가능한 많은 수를 최대한 빠르게 SHA-256에 대입해야 남들보다 먼저 '논스'를 찾을 수 있기 때문이다.

비트코인 채굴자들이 SHA-256을 통해 실행하는 연산을 우리와 같은 일반인들도 간접적으로 체험해볼 방법이 있다. 미리 몇 가지 상황을 가정하고 아래에서 알려주는 방법을 통해 직접 채굴자가 되어 '논스'를 찾아보자.

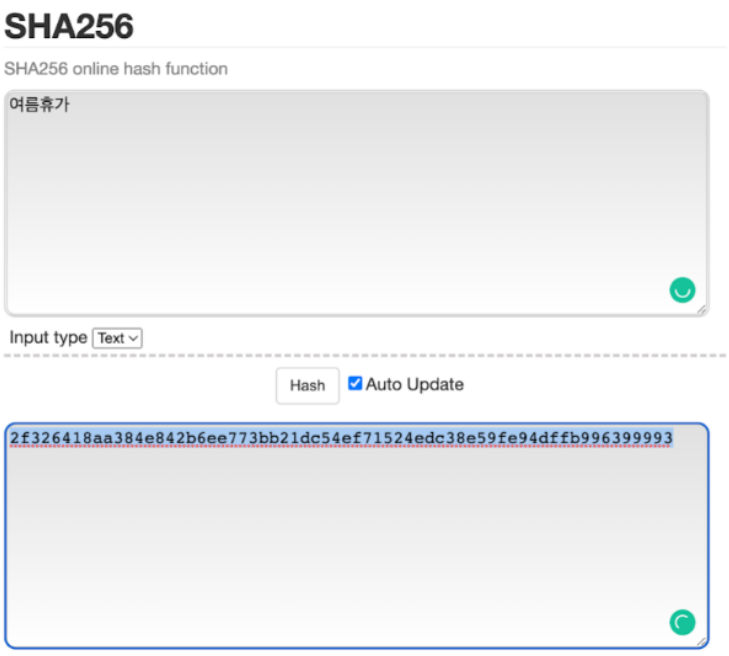
가정은 아래와 같다.

가정 1. 현재 비트코인 네트워크는 맨 앞에 '0' 3개가 연속으로 나오는 해시를 요구하고 있다.
가정 2. 블록에 담길 데이터는 '여름휴가'이다.

먼저 일반 텍스트를 SHA-256을 통해 16진수(Hexadecimal, 또는 Hex)로 바꿔주는 웹사이트에 접속한다. (링크: https://emn178.github.io/online-tools/sha256.html) 상단 영역에 '여름휴가'를 입력하면 하단에 숫자와 알파벳으로 구성된 기다란 16진수 문장이 나온다. 영어나 한국어 텍스트를 곧바로 2진수로 바꿀 수 없으므로 먼저 16진수로 바꾸는 과정이라 생각하면 된다.

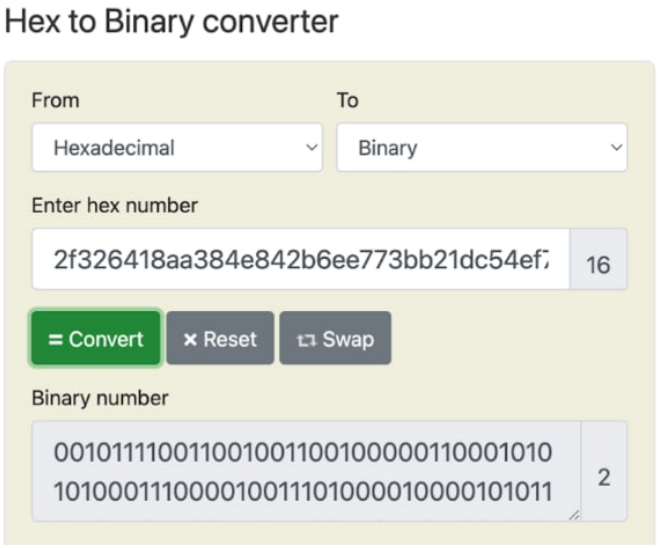
'여름휴가'를 입력하면 16진수 문장이 나온다.

SHA-256을 통해 '여름 휴가'를 16진수(Hex)로 변환



그 다음은 16진수를 2진수로 바꿔주는 두번째 웹사이트로 이동해야 한다. (링크:https://www.rapidtables.com/convert/number/hex-to-binary.html). 앞 웹사이트에서 구한 16진수 문장을 복사해 가져와 'Enter hex number' 밑 빈칸에 붙여넣기 한다. 그리고 'Convert' 버튼을 누르면 256개의 '0'과 '1'로 이루어진 2진수(Binary) 문장이 나온다.

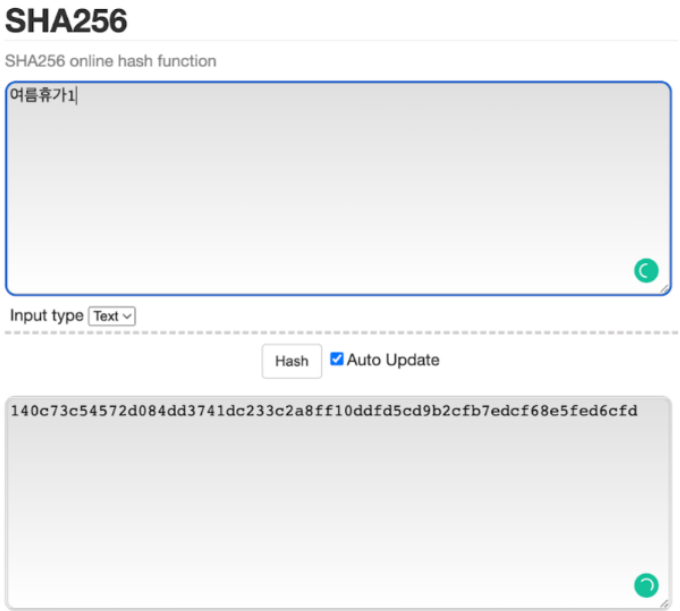
16진수(Hex)를 2진수(Binary)로 변환



앞전 웹사이트에서 얻은 16진수를 2진수로 변환하여 '해시'를 구하자.

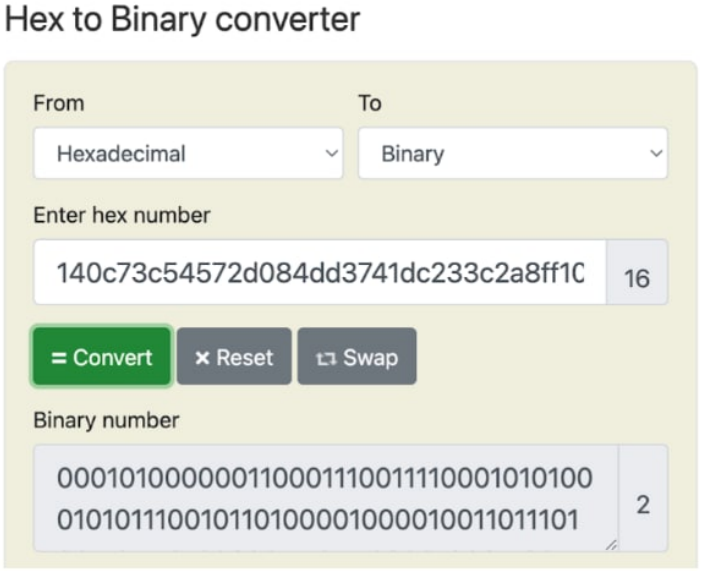
그런데 맨 앞에 '0'이 두 개밖에 없다. 비트코인 네트워크가 요구하는 해시는 '0'이 세 개 연속으로 나와야 하므로 계산 잘못했다. 다시 맨 앞으로 돌아가 이번엔 '여름휴가1'을 입력하여 16진수로 변환해 보자.

앞의 과정을 반복하며 논스를 유추



이 16진수를 두 번째 웹사이트로 복사해와 붙여넣고 'Convert' 하면 앞과 다른 2진수 값이 나오는 것을 알 수 있다. 이번에는 '0'이 맨 앞에 세 번 연속으로 나왔다. 빙고! 논스를 찾았다.

16진수를 2진수로 변환



비트코인 네트워크의 경쟁 환경은 채굴 산업의 성장을 도모

위 예시에서 단 두 번의 시도 만에 논스를 찾았으므로 19개의 0이 연속으로 나오는 논스도 쉽게 찾을 수 있으리라 생각하면 안 된다. 19개의 0이 연속으로 나올 확률은 0.00019%에 불과하다. 이 낮은 확률을 뚫고 정답을 찾기 위해 엄청난 설비투자를 단행하는 리스크를 감수하는 사람들이 바로 채굴자들이다.

시장경제에서 경쟁은 혁신을 일으키고 성장을 끌어낸다. 채굴자들은 비트코인 네트워크가 요구하는 '0'의 개수가 많아질수록 더 큰 규모의 설비투자가 필요할 뿐만 아니라 운영, 관리 측면에서도 높은 혁신을 이뤄내야 경쟁에서 살아남을 수 있다. 비트코인 채굴이 큰 규모의 산업으로 발돋움하고 있는 이유는 바로 비트코인 네트워크가 만들어낸 경쟁환경 덕분이라 해도 과언이 아니다.

그동안 비트코인 채굴은 높은 에너지 사용량 때문에 환경오염의 주범으로 공격받을 때 미디어에 잠깐씩 등장했을 뿐, 국내 암호화폐 투자자들에게 크게 관심을 받지 못했다. 만약 이 글을 읽는 여러분이 위에서 알려준 방법대로 비트코인 채굴자들이 하는 일을 간접적으로 체험해 봤다면, 그 일을 훨씬 커다란 규모와 높은 효율로 실행하고 있는 비트코인 채굴 기업들에도 관심을 가져보면 좋겠다. 어쩌면 그로 인해 비트코인에 투자해야 할 이유가 더욱 명확해질 수 있다.