HOW BITCOIN MINING WORKS

MorCryp

HOW BITCOIN MINING WORKS

When you hear about bitcoin “mining,” you envisage coins being dug out of the ground. But bitcoin isn’t physical, so why do we call it mining?

Because it’s similar to gold mining in that the bitcoins exist in the protocol’s design (just as the gold exists underground), but they haven’t been brought out into the light yet (just as the gold hasn’t yet been dug up). The bitcoin protocol stipulates that 21 million bitcoins will exist at some point. What “miners” do is bring them out into the light, a few at a time.

They get to do this as a reward for creating blocks of validated transactions and including them in the blockchain.

NODES

Backtracking a bit, let’s talk about “nodes.” A node is a powerful computer that runs the bitcoin software and helps to keep bitcoin running by participating in the relay of information. Anyone can run a node, you just download the bitcoin software (free) and leave a certain port open (the drawback is that it consumes energy and storage space - the network at time of writing takes up about 145GB). Nodes spread bitcoin transactions around the network. One node will send information to a few nodes that it knows, who will relay the information to nodes that they know, etc. That way it ends up getting around the whole network pretty quickly.

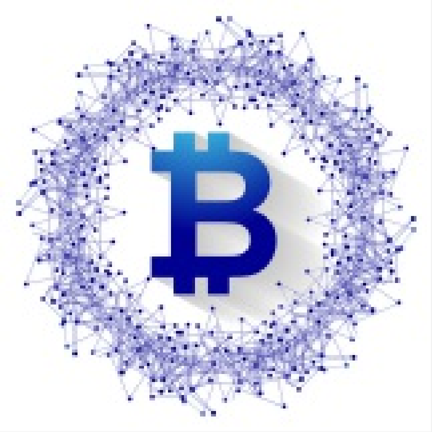
Some nodes are mining nodes (usually referred to as “miners”). These group outstanding transactions into blocks and add them to the blockchain. How do they do this? By solving a complex mathematical puzzle that is part of the bitcoin program, and including the answer in the block. The puzzle that needs solving is to find a number that, when combined with the data in the block and passed through a hash function, produces a result that is within a certain range. This is much harder than it sounds.

(For trivia lovers, this number is called a “nonce”, which is a concatenation of “number used once.” In the case of bitcoin, the nonce is an integer between 0 and 4,294,967,296.)

SOLVING THE PUZZLE

How do they find this number? By guessing at random. The hash function makes it impossible to predict what the output will be. So, miners guess the mystery number and apply the hash function to the combination of that guessed number and the data in the block. The resulting hash has to start with a pre-established number of zeroes. There's no way of knowing which number will work, because two consecutive integers will give wildly varying results. What's more, there may be several nonces that produce the desired result, or there may be none (in which case the miners keep trying, but with a different block configuration).

The first miner to get a resulting hash within the desired range announces its victory to the rest of the network. All the other miners immediately stop work on that block and start trying to figure out the mystery number for the next one. As a reward for its work, the victorious miner gets some new bitcoin.



ECONOMICS

At the time of writing, the reward is 12.5 bitcoins, which at time of writing is worth almost $200,000.

Although it's not nearly as cushy a deal as it sounds. There are a lot of mining nodes competing for that reward, and it is a question of luck and computing power (the more guessing calculations you can perform, the luckier you are).

Also, the costs of being a mining node are considerable, not only because of the powerful hardware needed (if you have a faster processor than your competitors, you have a better chance of finding the correct number before they do), but also because of the large amounts of electricity that running these processors consumes.

And, the number of bitcoins awarded as a reward for solving the puzzle will decrease. It's 12.5 now, but it halves every four years or so (the next one is expected in 2020-21). The value of bitcoin relative to cost of electricity and hardware could go up over the next few years to partially compensate this reduction, but it's not certain.

DIFFICULTY

The difficulty of the calculation (the required number of zeroes at the beginning of the hash string) is adjusted frequently, so that it takes on average about 10 minutes to process a block.

Why 10 minutes? That is the amount of time that the bitcoin developers think is necessary for a steady and diminishing flow of new coins until the maximum number of 21 million is reached (expected some time in 2140).

If you've made it this far, then congratulations! There is still so much more to explain about the system, but at least now you have an idea of the broad outline of the genius of the programming and the concept. For the first time we have a system that allows for convenient digital transfers in a decentralized, trust-free and tamper-proof way. The repercussions could be huge.