How does Bitcoin Mining Work?

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?

Similar to gold mining, 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 a maximum of 21 million bitcoins will exist at some point. What miners do is bring them out into the light, a few at a time. Once miners finish mining all these coins, there won’t be more coins rolling out unless the bitcoin protocol changes to allow for a larger supply. Miners get paid in transaction fees for creating blocks of validated transactions and including them in the blockchain.

To understand how bitcoin mining works, let’s backtrack a little bit and talk about **nodes**. A node is a powerful computer that runs the bitcoin software and fully validates transactions and blocks. Since the bitcoin network is decentralized these nodes are collectively responsible for confirming pending transactions.
Anyone can run a node—you just download the free bitcoin software. The drawback is that it consumes energy and storage space – the network at time of writing takes hundreds of gigabytes of data. 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, the pending transaction ends up getting around the whole network pretty quickly.
Some nodes are mining nodes,usually referred to as **miners**. These chunk 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 (which converts input data of any size into output data of a fixed length, produces a result that is within a certain range.

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

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 starts with a certain 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 that case, the miners keep trying but with a different block configuration.

The difficulty of the calculation (the required number of zeros 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).

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.

At the time of writing, the reward is 6.25 bitcoins per block, which is worth around $56,000 in June 2020.

However, it’s not nearly as cushy a deal as it sounds. There are a lot of mining nodes competing for that reward, and the more computing power you have and 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, but also because of the large amounts of electricity consumed by these processors.

And, the number of bitcoins awarded as a reward for solving the puzzle will decrease. It’s 6.25 now, but it halves every four years or so (the next one is expected in 2024). The value of bitcoin relative to cost of electricity and hardware could go up over the next few years to partially compensate for this reduction, but it’s not certain.

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.