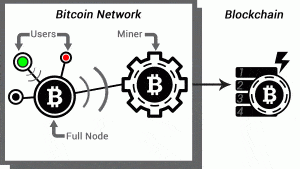
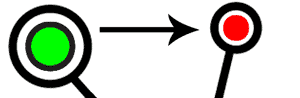
## **A Refresher - How Does Bitcoin Mining Work?**

This simplified illustration is helpful to explanation:



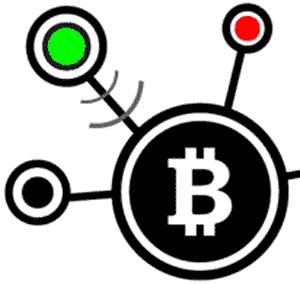
### 1) Spending

Let’s say the *Green* user wants to buy some goods from the *Red* user. Green sends 1 bitcoin to Red.



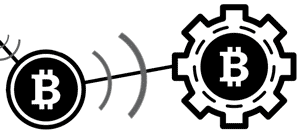
### 2) Announcement

Green’s wallet announces a 1 bitcoin payment to Red’s wallet. This information, known as transaction (and sometimes abbreviated as “ *tx*”) is broadcast to as many *Full Nodes* as connect with Green’s wallet – typically 8. A full node is a special, transaction-relaying wallet which maintains a current copy of the entire blockchain.



### 3) Propagation

Full Nodes then check Green’s spend against other pending transactions. If there are no conflicts (e.g. Green didn’t try to cheat by sending the exact same coins to Red and a third user), full nodes broadcast the transaction across the Bitcoin network. At this point, the transaction has not yet entered the *Blockchain*. Red would be taking a big risk by sending any goods to Green before the transaction is confirmed. So how do transactions get confirmed? This is where *Miners* enter the picture.



### 4) Processing by Miners

Miners, like full nodes, maintain a complete copy of the blockchain and monitor the network for newly-announced transactions. Green’s transaction may in fact reach a miner directly, without being relayed through a full node. In either case, a miner then performs work in an attempt to fit all new, valid transactions into the current block.

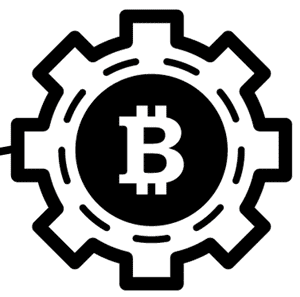
Miners race each other to complete the work, which is to “package” the current block so that it’s acceptable to the rest of the network. Acceptable blocks include a solution to a [*Proof of Work*](https://en.bitcoin.it/wiki/Proof_of_work) computational problem, known as a[*hash*](https://en.wikipedia.org/wiki/Hash_function) *.* The more computing power a miner controls, the higher their hashrate and the greater their odds of solving the current block.

But why do miners invest in [expensive computing hardware](https://www.buybitcoinworldwide.com/mining/hardware/) and race each other to solve blocks? Because, as a reward for verifying and recording everyone’s transactions, miners receive a substantial Bitcoin reward for every solved block!

And what is a hash? Well, try entering all the characters in the above paragraph, from “But” to “block!” into [this hashing utility.](http://www.fileformat.info/tool/hash.htm) If you pasted correctly – as a string hash with no spaces after the exclamation mark – the SHA-256 algorithm used in Bitcoin should produce:

“6afc21238f2d33e24e168195888721dd5ace05d76196671d6739789af92201ed.”

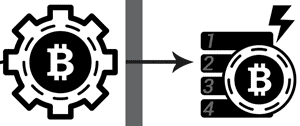
If the characters are altered even slightly, the result won’t match. So, a hash is a way to verify any amount of data is accurate. To solve a block, miners modify non-transaction data in the current block such that their hash result begins with a certain number (according to the current *Difficulty*, covered below) of zeroes. If you manually modify the string until you get a 0… result, you’ll soon see why this is considered “Proof of Work!”



### 5) Blockchain Confirmation

The first miner to solve the block containing Green’s payment to Red announces the newly-solved block to the network. If other full nodes agree the block is valid, the new block is added to the blockchain and the entire process begins afresh. Once recorded in the blockchain, Green’s payment goes from pending to confirmed status.

Red may now consider sending the goods to Green. However, the more new blocks are layered atop the one containing Green’s payment, the harder to reverse that transaction becomes. For significant sums of money, it’s recommended to wait for at least 6 confirmations. Given new blocks are produced on average every ten minutes; the wait shouldn’t take much longer than an hour.



## The Longest Valid Chain

You may have heard that Bitcoin transactions are irreversible, so why is it advised to await several confirmations? The answer is somewhat complex and requires a solid understanding of the above mining process:

Let’s imagine two miners, *A* in China and *B* in Iceland, who solve the current block at roughly the same time. A’s block (*A1*) propagates through the internet from Beijing, reaching nodes in the East. B’s block (*B1*) is first to reach nodes in the West. There are now two competing versions of the blockchain!

Which blockchain prevails? Quite simply, the *longest valid chain* becomes the official version of events. So, let’s say the next miner to solve a block adds it to B’s chain, creating B2. If *B2* propagates across the entire network before *A2* is found, then B’s chain is the clear winner. A loses his mining reward and fees, which only exist on the invalidated *A* -chain.

Going back to the example of Green’s payment to Red, let’s say this transaction was included by A but rejected by B, who demands a higher fee than was included by Green. If B’s chain wins then Green’s transaction won’t appear in the B chain – it will be as if the funds never left Green’s wallet.

Although such blockchain splits are rare, they’re a credible risk. The more confirmations have passed, the safer a transaction is considered. This is why what is known as '0-conf' or "0 confirmations" on the Bitcoin Cash blockchain is so dangerous.