A Gentle Introduction To Bitcoin Mining

BRAVE NEWCOIN.
Digital Currency Insights

Table of Contents

A Gentle Introduction To Bitcoin Mining

Authored By

Antony Lewis

Antony Lewis has a passion for virtual currencies such as bitcoin, and the underlying technologies behind them, including blockchain data structures and distributed consensus systems. Antony believes that these new ways of putting the technologies together will change the world of business, reminiscent of how the internet changed the distribution of information. Antony consults businesses, helping them understand the implications of blockchain technology.

antony@bitsonblocks.net

@antony_btc

Published By

BraveNewCoin

BNC.
Digital Currency Insights

Adapted from

Bits On Blocks

The '**Gentle Introduction Reference Papers™** are the first in a series of accessible documents published by Brave New Coin for industry decision makers. Designed to demystify the inner workings of Bitcoin, Digital Currencies and the emerging Blockchain technology.

Series ONE covers:

"A Gentle Introduction To"

> Bitcoin

> Blockchain Technology

> Bitcoin Mining

> Digital Tokens

Free to Download and Share

How Do Bitcoin Transactions Work?

The process is:

1. Make a payment (a bitcoin transaction)

2. Wait for it to be mined in a block (upto 10 mins on average)

3. Wait for more blocks to be mined on top (average 10 mins per block)

1. Make a payment. When you make a bitcoin payment, the transaction message is sent to the network, and passed around all the network participants (called 'nodes'). At this point the transaction is 'unconfirmed,' which means the nodes have seen that the payment has been initiated. They have validated it according to certain technical and business logic rules, but it isn't yet been written into anyone's bitcoin blockchain ledger.

Unconfirmed transaction = valid, known transaction, but not yet included in the ledger.

2. Wait for it to be mined in a block (upto 10 mins on average). Miners take the list of unconfirmed transactions (specifically, those that they know about), and they bundle them into a block, which is just a list of transactions plus some other data.

They then get to work 'mining' the block which means playing a guessing game to find a random number.

If they guess right, then the block is published to the rest of the network. The computers on the network validate that the block meets the criteria, and then ignore it or store it into their blockchains. The competition then starts again with the unconfirmed transactions that have accumulated since.

The network adjusts the difficulty the guessing game so that a block is created every 10 mins or so, irrespective of the amount of computing power in the network, or the number of transactions.

3. Wait for more blocks to be mined on top (average 10 mins per block). The next block is mined on top of the one with your transaction in. This new block will refer to the previous block (hence, 'blockchain'). The more blocks that have been built on top of the one with your transaction, the more 'baked' into the blockchain it is, and so the harder it is to unwind through block-reorganisation attacks.

Unconfirmed transaction -> Confirmed transaction (1 block) -> Confirmed transaction (many blocks)

The current advice suggests that after 6 blocks, the chances of the transaction being unwound is very small. IIf you are receiving a payment; the higher the value, the longer you may want to wait. This reduces risk, although the risk reduction achieved shows diminishing returns.

Why Is Mining Needed In Bitcoin?

There are two parts to this. First you need a way to get transactions into the ledger, secondly you need a way to make it expensive for malicious attackers to add dishonest blocks.

Ledger addition. Transactions are added to the ledger in blocks, creating a rough time order for the transactions. In bitcoin you can't trust the timestamp of any particular participant, and there is no 'master clock' to trust, so block order is the equivalent of time order.

Financial deterrent. This is about the guessing game, called "Proof of work". You don't actually need the guessing game to add blocks to a blockchain. However, the guessing game makes it computationally expensive (therefore financially expensive) to add blocks. This cost acts as a deterrent to attackers who would otherwise want to add dishonest blocks. So long as most of the network is 'honest', then the dishonest parties will have a tough time creating rogue blocks.

"Why proof of work?", in three acts:

Act 1

- Anyone can create blocks on an 'open' network.
- As you can't trust anyone specifically, each individual node has to assume that the 'majority' of the rest of the network is right.
- To dominate the network, you need to create many aliases who are all under your control and all agree with each other. This kind of domination-by-numbers is called a 'Sybil attack'.

Act 2

- It is cheap and easy to spawn validators who all agree with each other.
- Therefore it is very cheap to bully the network.
- For a network to be secure against this, you need to have a more expensive way to bully the network.

Act 3

- Computational power is more expensive, it requires investment and upkeep.
- Therefore use majority-by-computational-power instead of majority-by-numbers.
- Malicious players will need to spend a lot more money to dominate the network.

Finale

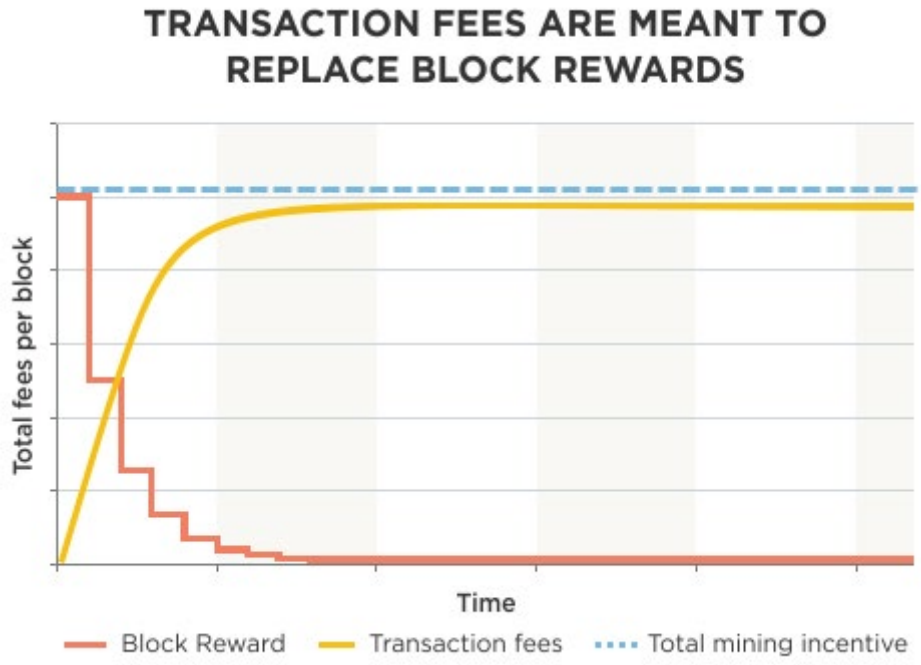
- The name given to a challenge that is computationally expensive for the sake of it, is called a "**Proof of work**" challenge.

Why Do Miners Mine?

Mining reward = Voluntary transaction fees + Block reward (currently 25 BTC per block)

When you mine a block, you get to collect any voluntary transaction fees from the transactions you have included. You also get to write one transaction paying yourself some BTC (currently 25 BTC, and reducing to 12.5 BTC in the middle of 2016). This is called a 'block reward' or 'coinbase transaction' (not to be confused with the American company called "Coinbase" which operates under a UK legal entity "Coinbase UK, Ltd").

This is the 'mining process' i.e. how bitcoins are created. The reward decreases with time, and in theory, transaction fees will replace the block reward.



Transaction fees are not mandatory (hence the "bitcoin transactions are free" mantra) but miners will seek out transactions containing fees, and preferentially add them to blocks that they are creating. If there are more unconfirmed transactions than can fit in a block, rational miners will mine the ones with the highest transaction fees first.

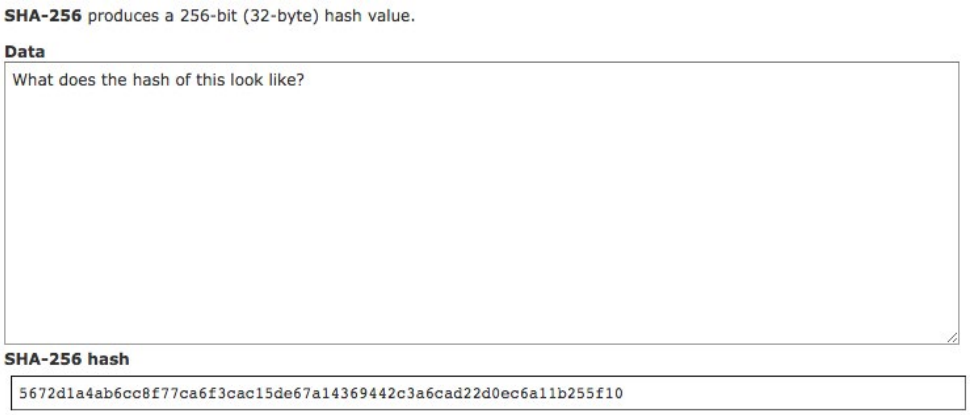
What Is This 'Computationally Expensive' Guessing Game?

Miners use a lot of computing power trying to guess a number which, when added to a block and put through an algorithm, outputs a 'hash' that meets certain criteria.

A hash is a fingerprint of data. It's easy to make a hash from some data, but computationally impossible to create the data from the hash. Hashes look random compared with the data put in.

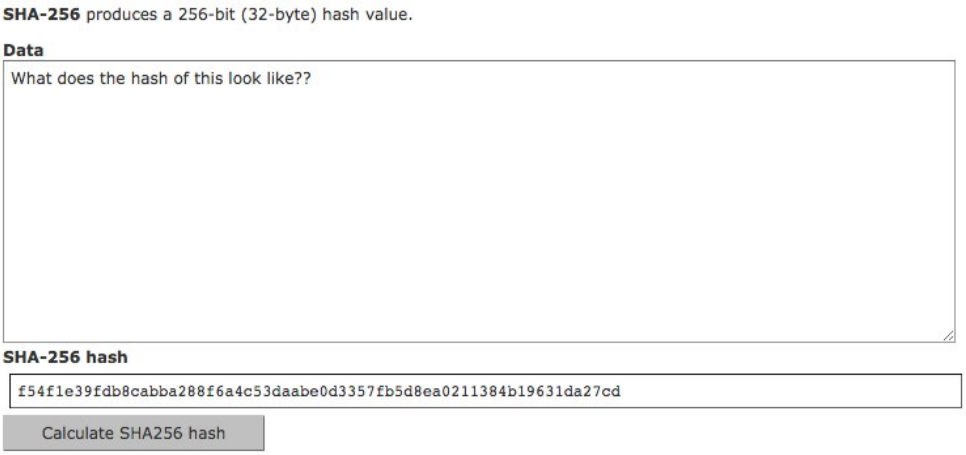
You can play with hashing here:

http://www.xorbin.com/tools/sha256-hash-calculator and type some data into the big box. You'll see the hash in the smaller box. I typed "What does the hash of this look like?":



It's easy to generate a hash from some text, but impossible to re-generate the text from the hash.

If you change just one part of the data, the hash looks entirely different. I added a question mark:



Adding or changing just one character results in a totally different-looking hash.

What Is This 'Computationally Expensive' Guessing Game?

The mining challenge: By changing the data slightly, try to find a hash starting with 0000000.

By adding "-17" to the end of the sentence, you can find a hash beginning with one zero:

Input: "What does the hash of this look like?-17"

Hash: **0fd82107e6e73b6f369853da3b53d4a93e8be1e5b3a4dd7da2b4ea644774bc80**

By continuing more trials, the first time a hash appears starting with a double zero is with -272 appended:

Input: "What does the hash of this look like?-272"

Hash: **00629a604a7ec6b1f05e7703c57197ed6119a6282e9b5f750e14a1500578d3fd**

Bitcoin block mining. Bitcoin mining is essentially the same game, where you tweak the input data (the block header) until you get an output hash that matches what is required by the network at that point in time.

A recent bitcoin block (#372910) was 'solved' with the hash;

00000000000000000b037a61e47df14b035199b5a2d464691b9456394bc07da

This had enough zeroes to satisfy the network at this time*.

**More accurately the block header containing the nonce is hashed twice using the SHA-256 hashing algorithm, and had to meet a number smaller than the target number determined by the network difficulty of 54,256,630,327.89 (at block #372910).*

Who Mines?

Satoshi Nakamoto, the proposer of bitcoin, recognised that if you want lots of people to use hardware and energy creating this network, you need to incentivise them: i.e. you need to pay them. The white paper can be read here.

How do you pay anonymous participants without creating some sort of power structure? A source of funding provided by an entity (e.g. if a company or government paid miners) would give that entity censorship rights and some control over who mined, and what gets mined.

Satoshi realised that an intrinsic source of funding, where a payment is paid by the system rather than by any external party, was the answer. This is why miners are paid by the system, in tokens which have a value that is related to the size and security of the system. Theoretically, the more valuable the tokens become, the more money can be spent mining, leading to an increase in security and an increase in the value of the network.

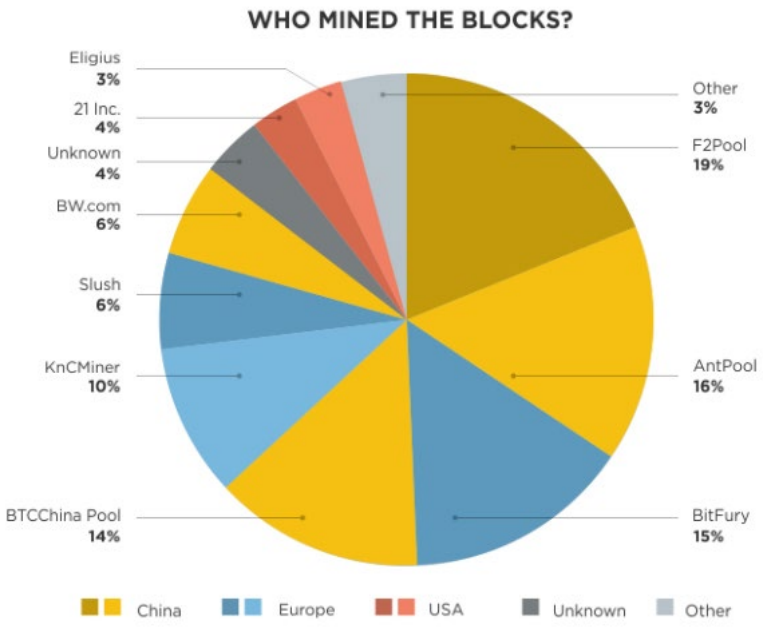
Anyone can "participate" in the mining activity, you just need to download the software and run it. Your computer will then start taking transactions that it receives through the bitcoin network, and it will bundle them into blocks, and start mining the block.

Your chance of mining a block is some what proportional to the amount of **computing power** you throw at it, because mining is a guessing game, and faster computers guess more quickly. It is also related to **how fast your internet connection is**. Once you have created a valid block, you want to make sure that it's incorporated quickly, before someone else with a faster internet connection distributes his block.

In practice, successful miners form groups, or pools, and combine their processing power. If they win a block, the reward gets shared between participants. This is similar to forming a lottery syndicate, so you win less, but more often, and your income becomes lumpy.

Currently, the top 10 mining pools consistently create about 90% of the blocks, and China-based pools create more than 60%. Pools are generally controlled by the "pool operator" which is a person or a few people. So, despite the rhetoric of bitcoin being decentralised, it is controlled by a handful of people in China.

The decentralisation of bitcoin, although romantic in theory, doesn't seem to be working properly in practice.

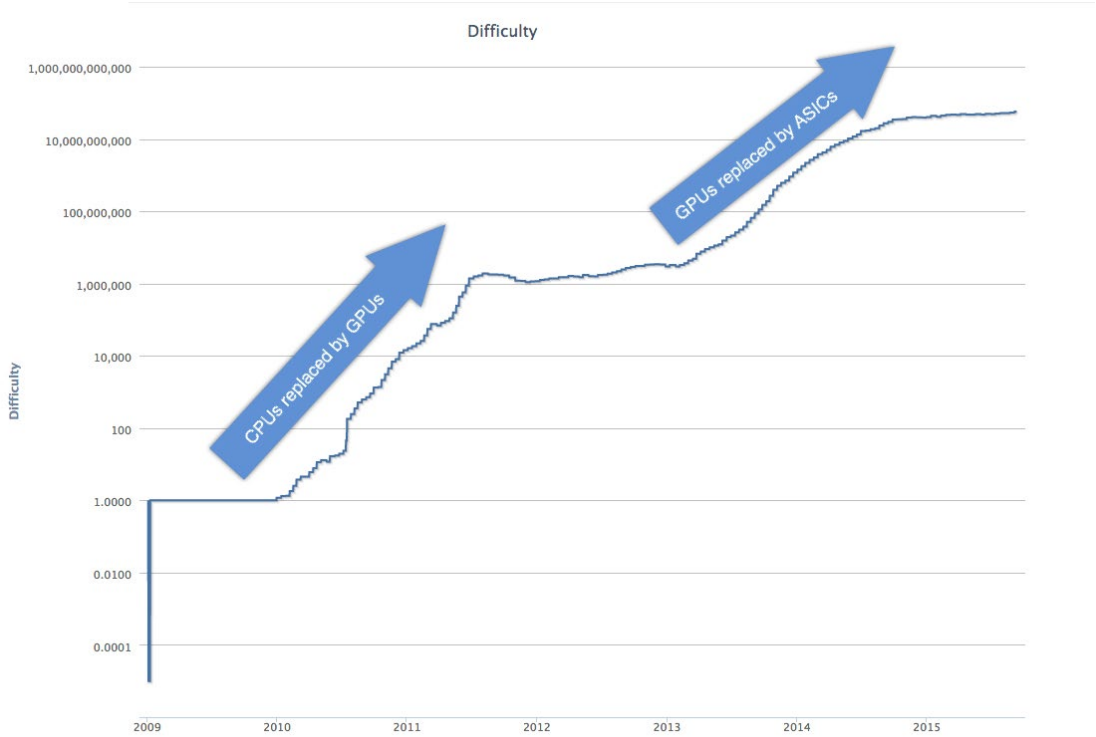


Mining is mainly done by Chinese pools. 4 days worth of mining in early Sep 2015

A Very Brief History Of Mining

In 2009, people could mine successfully on their laptops and home computers, using the CPU (Central Processing Unit) to do the calculations. There seemed to be a gentleman's agreement not to use more powerful GPUs (Graphics Processing Unit, the proccessing chips that display your monitor and laptop screens) that were more efficient and faster at running this specific calculation, but harder to set up. However that gentleman's agreement seems to have broken down, and GPU mining made CPU mining obsolete, driving a large increase in mining difficulty between 2010-12.

As the price of bitcoin and so the value of the reward increased, people started investing in mining equipment, and began manufacturing chips called ASICs (Application-Specific Integrated Circuits). These are good for nothing except hashing / mining (so take popular comparisons with the world's supercomputers with a pinch of salt). This was the next revolution in hashing power, starting in 2013.



What Can And Can't Attackers Do?

A dishonest miner can:

1. Refuse to relay valid transactions to other nodes.

2. Attempt to create blocks that include, or exclude, specific transactions of his choosing.

3. Attempt to create a 'longer chain' of blocks, which makes previously accepted blocks become 'orphans' and not part of the main chain.

He can't:

1. Create bitcoins out of thin air.*

2. Steal bitcoins from your account.

3. Make payments on your behalf or pretend to be you.

*Well, he can, but only his version of the ledger will have this transactions. Other nodes will reject this, which is why it is important to confirm a transaction across a number of nodes.

With transactions, the effect a malicious attacker can have is very limited. If the rest of the network is honest, they will reject any invalid transactions coming from the attacker, and they will hear about valid transactions from other honest nodes, even if the attacker is refusing to pass them on.

With blocks, if the attacker has sufficient block creation power (and this is what it all hinges on), he can delay your transaction by refusing to include it in his blocks. However, your transaction will still be known by other honest nodes as an 'unconfirmed transaction', and it will eventually be included in one of their blocks.

Worse though, is if the attacker can create a longer chain of blocks than the rest of the network, and can invoke the "longest chain rule". This lets them unwind a transaction.

Here's how:

1. Create two payments with the same bitcoins: one to an online retailer, the other to yourself (another address you control).

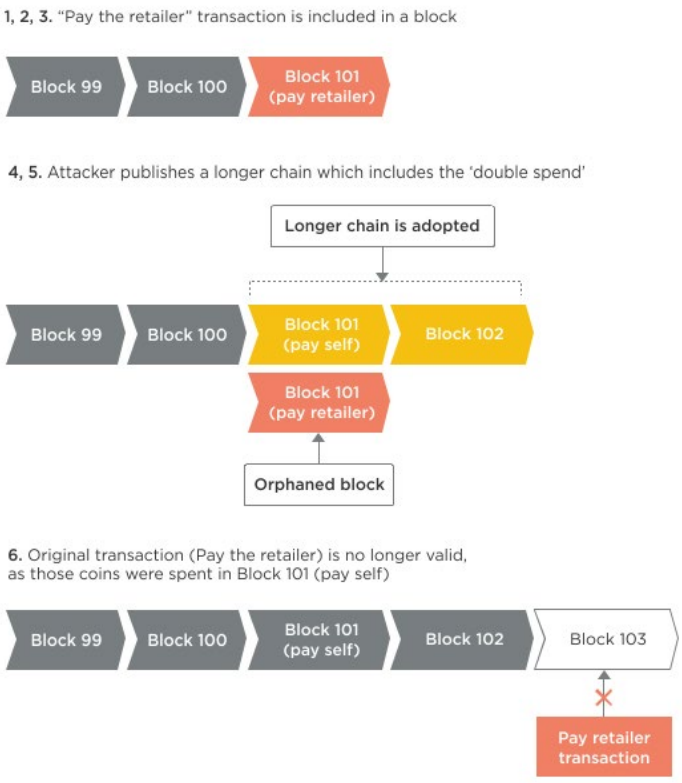
2. Only broadcast the payment to the retailer.

3. When the payment gets added to an honest block, the retailer sends you goods.

4. Secretly create a longer chain of blocks which swaps out the payment to the retailer, and swaps in the payment to yourself.

5. Publish the longer chain. If the other nodes are playing by the "longest chain rule" rule, they will ignore the honest block with the retailer payment, and continue to build on your longer chain. The honest block is said to be 'orphaned' and does not exist to all intents and purposes.

6. The original payment to the retailer will be deemed invalid by the honest nodes because those bitcoins have already been spent (in your longer chain).



This is called a "double spend," as the same bitcoins were spent twice – but the second one was the one that became part of the eventual blockchain.

CONCLUSION

To conclude, bitcoin mining is the theoretically decentralised process where anyone can add a block of transactions to the bitcoin blockchain, without needing permission from any authority, and getting paid in bitcoins for it. It is made deliberately difficult, using proof of work as a defence against Sybil attacks. The mining difficulty increases with the network hashing power, so the more processing power across the whole network, the, the more power someone needs to assert control over the network.

It works well until any entity or coordinated group controls too much of the hashing power, at which point they can control various aspects of the system. Currently 90% of blocks are mined by known 'pools' or syndicates of miners, and if a few pools join together, they could effect changes and assert control over the network.

Puzzled by some of the terms used in these gentle introduction series. Please visit our glossary for a complete terminology breakdown.

www.bravenewcoin.com/bitcoin-basics/glossary/

About

BNC.
Digital Currency Insights

Brave New Coin is a Data & Research company focused on the exponential Blockchain & Digital Equities industry. We collect, index and report on countless digital assets and their market & industry activities.

Subscribe to our weekly newsletters to keep in the loop with industry news.

Subscribe

www.bravenewcoin.com

contact@bravenewcoin.com

Explore more resources

- Research & insights
- Market-Data
- Developer tools (API's)

Bits on Blocks is a Singapore - based blog, run by Antony Lewis, who focuses on Blockchain Technology. Mr Lewis believes that Blockchain Technology can make the world a better place.

antony@bitsonblocks.net

www.bitsonblocks.net