Factual information about bitcoin

by Gregg Ink

How could something purely digital ever be worth anything?

Version 1.0.1

Disclaimer
Some concepts have been simplified in order to make them easier to understand to the general public but they are correct in essence. The author accepts no responsibility in the event that mistakes lead to loss or damage.

Understanding the big picture begins with hashing.

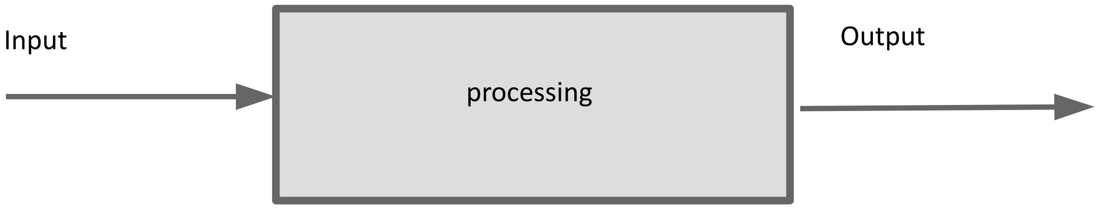
How could bitcoin be worth anything? How does that even make sense? It is purely digital. There is nothing physical to see or touch. How can you turn thin air into money?

Understanding the technical details does not come easily for everybody, especially those not technically inclined. But it is important to at least understand the big picture in order to think about bitcoin clearly and intelligently.

Before we can understand bitcoin, we need to understand hashing. So what is hashing? Firstly, hashing is an algorithm. An algorithm is a series of steps to be performed in order to achieve a particular goal. We can take the example of calculating the average of two numbers. To calculate the average of two numbers one needs to add them up and divide the sum by two. The adding and dividing are the steps which need to be performed in order to achieve the goal i.e. calculating the average.

An algorithm is a series of steps to be performed in order to achieve a particular result.

Every algorithm can be thought of as a system and every system has this basic structure: there is an input, processing and output.



Thinking back about our example of the average of two numbers. The input would be our two numbers (let’s say 5 and 3). The processing would be the addition and division by two. The output would be our actual average (which is 4).

There are many different types of hashing algorithms but the one we will concern ourselves with is SHA256 because that’s the engine of bitcoin.

Computers internally do not use numbers in the form we are most familiar with but handle only zeroes and ones. A single zero or a single one is called a bit. The bit is the smallest unit of information that a computer can handle. For convenience bits are grouped in bundles of 8 which we call bytes. The output of the SHA256 algorithm is always 32 bytes or 256 bits in length, hence the name. SHA stands for Secure Hashing Algorithm. The output of SHA256 is called a hash.

The input of SHA256 can be any data that you can store on a computer. It can be a text, an e-mail, an image or a movie. It can be short or long; any arbitrary length.

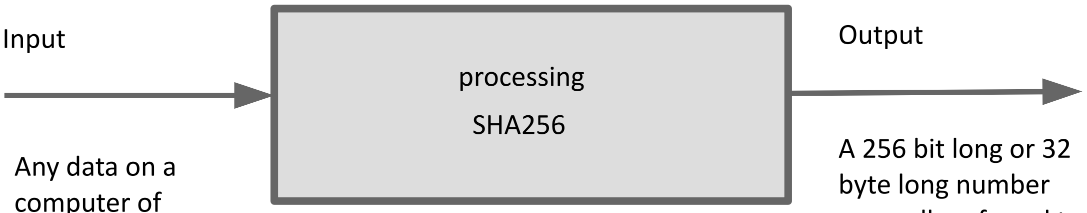
The processing that occurs during SHA256 is long and complicated. It is really beyond the scope of this discussion. There is however nothing secret about it. You can google it and find out exactly what SHA256 does if you are interested. It doesn't really matter what it does, however three properties are very important.

1. SHA is deterministic. This means that exactly the same input will lead to exactly the same output every time.

2. It is irreversible. That means that if I tell you the output, there is no way for you to tell what the input was. You can try to find out through trial and error but since the input could be anything, if you don't have a hint of what it might be, that's a hopeless technique. It might seem surprising to some that an algorithm about which the steps are known could be irreversible but that's not really so strange. Let's go back to our example of the average. If I tell you what the output is, can you tell what the input was? If you know that the average was 4, then the input could have been 5 and 3 or 88 and -80 or 1 and 7, etc.

3. A slight change in the input leads to a completely different output. That's really a consequence of the second property. It ensures that you cannot hone in on a particular target output by continuously tweaking the input.

SHA256



Input

processing

SHA256

Output

Any data on a computer of arbitrary length:
* a text
* a movie
* etc.

A 256 bit long or 32 byte long number generally referred to as a ‘hash’

Properties:
1. Deterministic
2. Irreversible
3. Slight change in input -> totally different output

A small bit about numbers

Denary numbers
We use 10 numerals for the numbers we use day to day, namely 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. What do you after nine? You have run out of numerals so you simply recycle the ones that you have already used and add an extra digit to the number. So it continues: 10, 11, 12, ... Those numbers are known as denary numbers.

Binary numbers
Computers, inside their chip, don't use denary numbers. They use only zero and one. So how do they represent the number two? Well it needs to recycle the numerals already and add an extra digit. Two is being represented as 10.

Hexadecimal numbers.
But why stop there? Programmers often use 16 numerals. The first ten are the same and after that they use a, b, c, d, e and f. So the numbers go: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, 10, 11, 12, ...
These are known as hexadecimal numbers. They are convenient because they allow larger numbers to be represented with fewer digits.

It is important to note that all these are merely different ways of representing the same numbers and they are not special in any way. Seventeen can be written 17, 10001 or 11 as denary, binary and hexadecimal respectively.

Most of the time the context will make clear how numbers are being represented. It is common practice to add the prefix "0x" in front of hexadecimal numbers when the context is not enough. So the number 0x45 is definitely the number sixty-nine.

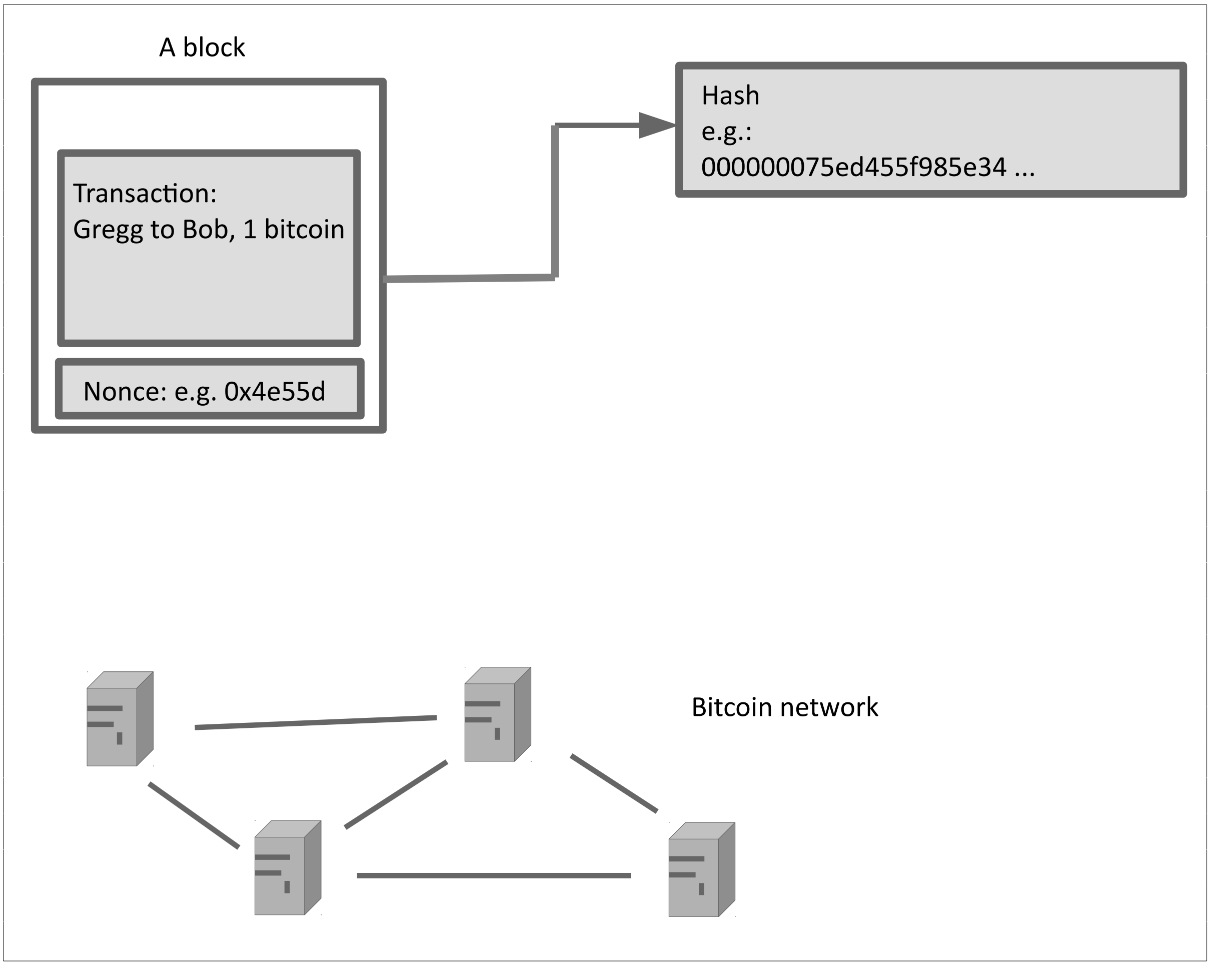
Hashes are always written in hexadecimal form so no prefix is necessary.

Making bitcoin happen

Okay. All that is fine and well but how does any of this make bitcoin happen?

Well, imagine I have a public ledger. A single page from this ledger shall be called a “block”. On this, I write transactions. Say I have one bitcoin and I send it to Bob. Now I have zero and Bob has one. More transactions are added to the block.

There is a network of computers owned by the bitcoin community that we shall call the “bitcoin network”. The people who own those computers shall be called the “miners”. They take the block and produce a hash using SHA256. The miners are trying to make the output of the hash fit certain constraints. How can they do that since the algorithm is deterministic? They add a nonce to the block. “Nonce” stands for “number used only once”. Changing that input a little will completely change the output. They are trying to produce a hash with a certain number of leading zeroes. Let’s say seven zeroes for example.

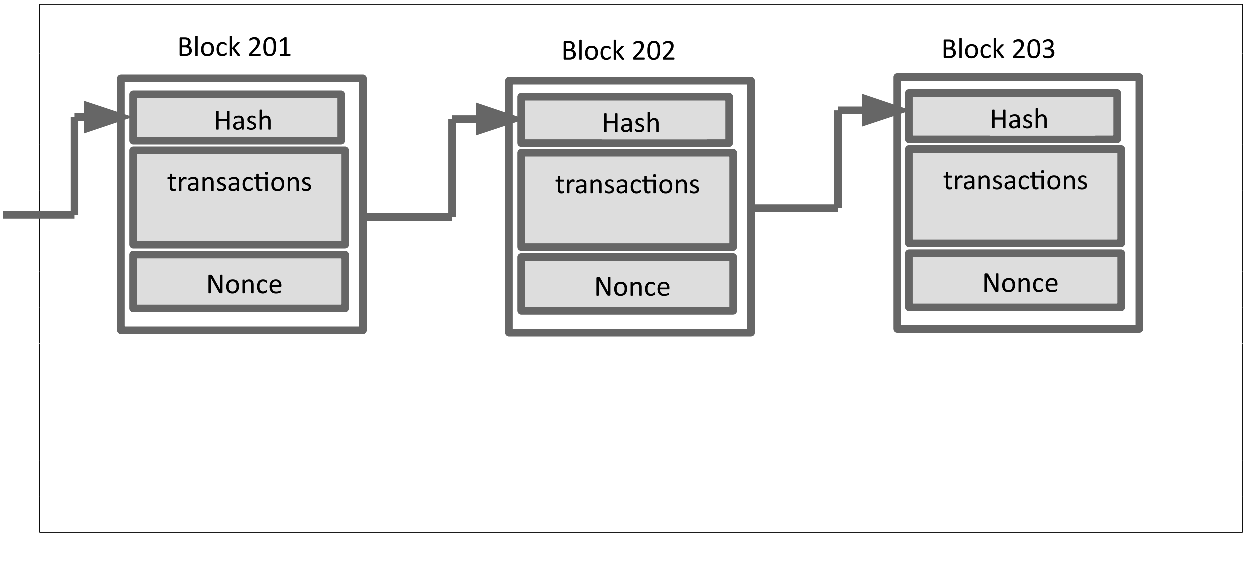


So they try one nonce after the other until one finds a nonce such that when added to the block, it produces an output with the required number of leading zeroes. It's a game of probability. It could be the first nonce you try, or you might have to try a billion times.

It's a competitive race where everyone is trying to be the first to find a good nonce. The more computing power you can bring to the table, the more likely you are to be the first to find it. Let's say John is the first miner to find a good nonce. He does broadcast his find to the rest of the network. Everyone can then check for themselves that the nonce is indeed correct and then John is acknowledged to be the first to find it. John is then said to have "mined" the block and as a reward he can pay himself 12.5 bitcoins. Those bitcoins come out of thin air into John's bitcoin wallet.

While the community was trying to mine the block, more transactions have happened and they were added to a queue. They are now used to fill the next block and the community gets mining again.

There is an important twist here though and this is what made bitcoin possible. Before bitcoin, people had been thinking for many years about digital currencies. There was a problem and it was called the double spending problem. How could you make sure that people wouldn't cheat and spend the same money twice? This twist is very simple but very powerful. You simple add the hash from the right nonce to the next block. Similarly the block just mined had the hash from the previous block. That's why the entire public ledger is called a blockchain. The hashes string the blocks together like in a chain.



Blockchain

A blockchain is the creation of an immutable digital record.

To work effectively two conditions are required:
1. A cryptographic hash of the previous block has to be carried through each and every block.
2. Several copies of the blockchain must exist in separate places that are not controlled by the same party. The more parties control a copy, the more reliable the blockchain.

So now imagine that I want to be malicious and pretend that I had ten bitcoins instead of one and after giving one to Bob I now have 9 left. Can I change the block after the fact? That doesn't work. Not only will I be unable to change every copy of the blockchain but the hashes would no longer add up. With every new block added to the chain, it gets much harder to change the data in a given block.

Rewards and difficulty

Why do miners mine? What do they get out of it? For each block a miner successfully mines, he receives a reward. The reward are bitcoins generated out of thin air and going into the bitcoin wallet of the miner. Right now the reward is 12.5 bitcoins per block. In addition the miner also gets the fees relating to the transactions in the block.

Every 210,000 blocks, which is about every 4 years, the reward is cut in half. In about three years from now the reward shall be 6.25 bitcoins per block. This will continue until a total of 21 million bitcoins have been mined. Then the miners will no longer receive rewards for the mining and will need to rely purely on the transaction fees as an incentive to mine.

Mining costs money. It takes electricity and an investment in hardware. The value of bitcoin is determined by supply and demand. When the value of bitcoin is high, many miners join the bitcoin network and compete for the reward of the next block. When the value of bitcoin goes down, miners drop out as they deem it no longer profitable to mine.

The more computing power (or hashing power as it's often referred to) there is in the network the sooner you might expect a good nonce to be found. But the bitcoin rules state that you should have a block roughly every 10 minutes. How does that work? The answer is that the difficulty is being adjusted. The more leading zeroes are required at the start of the hash, the harder it is the find the nonce.

Mining 2,016 blocks should take about two weeks. Every 2,016 blocks the miners check how long it actually took to mine the blocks and the difficulty is adjusted accordingly by increasing or reducing the number of leading zeroes required for each hash.

One can keep track of bitcoin rewards and halving times on www.bitcoinblockhalf.com.

Confirmations

If you have ever done a bitcoin transaction then you know that they are not instantaneous. There are a couple of reasons for that.

When you send your transaction, it goes into a queue. This queue is called the “mempool” by the community. Transactions are selected from the mempool to go into the next block but they are not necessarily selected in the order in which they were generated. The miners pick and choose the transactions with the highest transaction fee first. It is possible to volunteer higher transaction fees to see a transaction processed faster.

There is a new block about every 10 minutes. Thus, if the mempool is empty, that’s on average how long it will take to see a first confirmation of your transaction. One confirmation means your transaction is now in a mined block. Each subsequent block mined is an additional confirmation of your transaction.

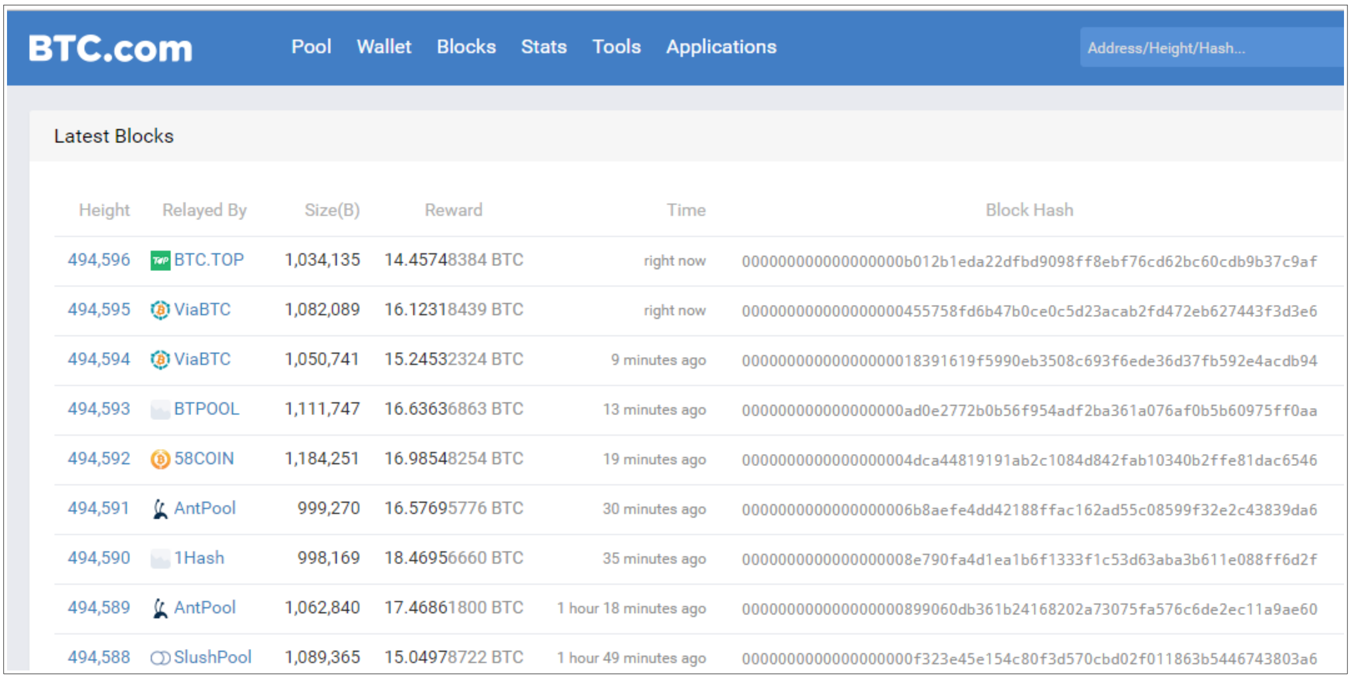
When blocks are mined there is always a very small chance that two miners will find a good nonce at the same time. They both get acknowledged as the miner of the block by about half the miners. Then the blockchain splits and the network is now working with two different versions of the blockchain. Subsequent blocks are only going to be accepted by half the miners. The rules state that miners should always accept the longest blockchain as the valid one. Those splits usually get resolved quickly and half the miners drop their version of the blockchain in favour of what has become the dominant version. That means that all transactions that happened in the “orphaned” blocks are null and void. The bitcoins are not lost. They are still in the original wallet and it’s as if those transactions never happened.

To avoid these problems it is common practice for a business to wait for 6 confirmations before considering a debt paid.

Looking at the blockchain

The blockchain is public information so anyone can look at it. I shall use the website btc.com as an example but this is by no means the only or best way to look at the blockchain. In fact, I encourage you to look at several websites and ensure yourself that indeed the blockchain is decentralized and every copy is identical. Examples of other websites are blockexplorer.com and blockchain.info. Looking at the blockchain could be a way of making some of the concepts more concrete and make them crystallize in your mind.

Let’s have a look at the screenshot below.



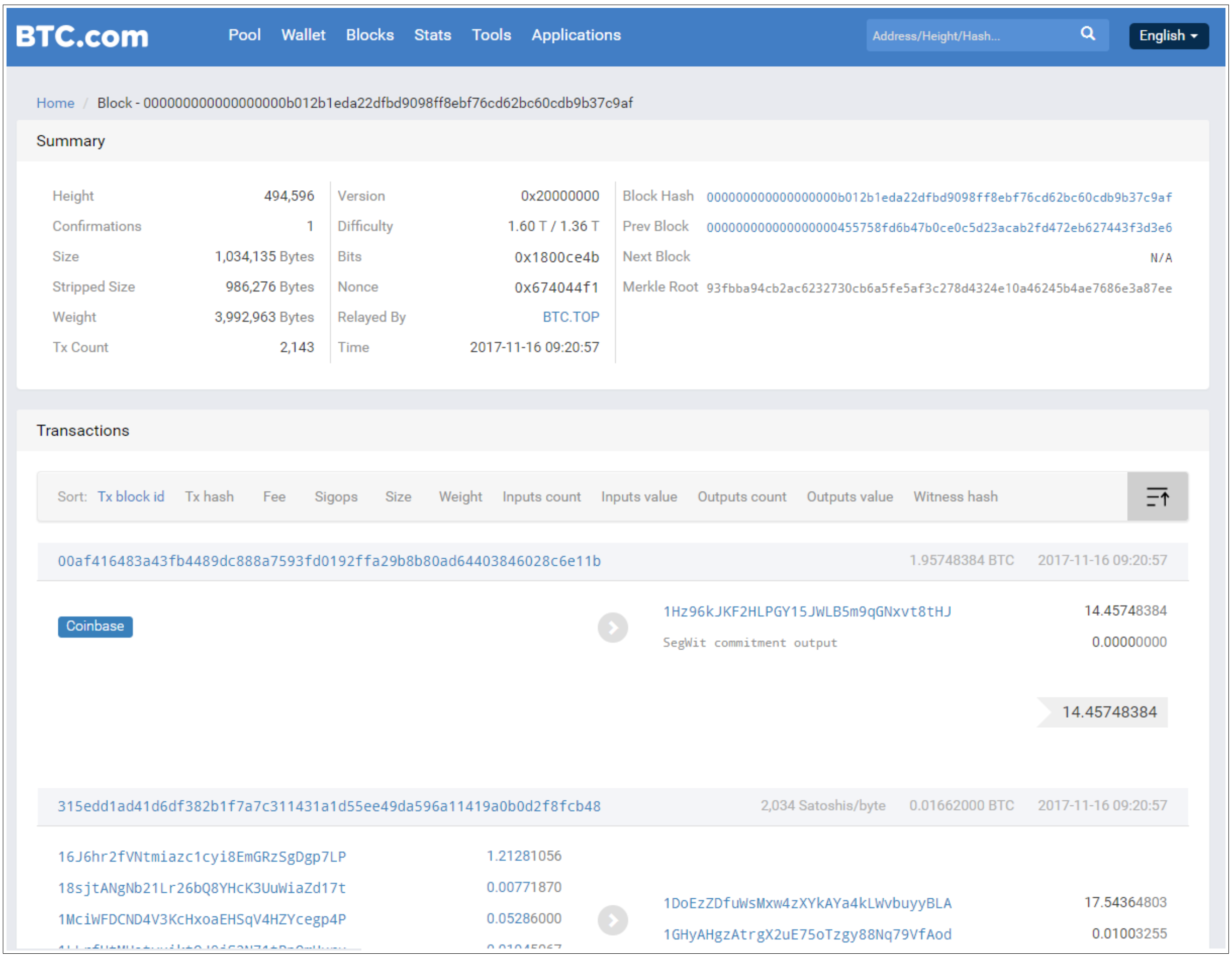
Latest Blocks

Height	Relayed By	Size(B)	Reward	Time	Block Hash
494,596	BTC.TOP	1,034,135	14.45748384 BTC	right now	000000000000000000b012b1eda22dfbd9098ff8ebf76cd62bc60cdb9b37c9af
494,595	ViaBTC	1,082,089	16.12318439 BTC	right now	000000000000000000455758fd6b47b0ce0c5d23acab2fd472eb627443f3d3e6
494,594	ViaBTC	1,050,741	15.24532324 BTC	9 minutes ago	00000000000000000018391619f5990eb3508c693f6ede36d37fb592e4acdb94
494,593	BTPOOL	1,111,747	16.63636863 BTC	13 minutes ago	000000000000000000ad0e2772b0b56f954adf2ba361a076af0b5b60975ff0aa
494,592	58COIN	1,184,251	16.98548254 BTC	19 minutes ago	0000000000000000004dca44819191ab2c1084d842fab10340b2ffe81dac6546
494,591	AntPool	999,270	16.57695776 BTC	30 minutes ago	0000000000000000006b8aefe4dd42188ffac162ad55c08599f32e2c43839da6
494,590	1Hash	998,169	18.46956660 BTC	35 minutes ago	0000000000000000008e790fa4d1ea1b6f1333f1c53d63aba3b611e088ff6d2f
494,589	AntPool	1,062,840	17.46861800 BTC	1 hour 18 minutes ago	000000000000000000899060db361b24168202a73075fa576c6de2ec11a9ae60
494,588	SlushPool	1,089,365	15.04978722 BTC	1 hour 49 minutes ago	0000000000000000000f323e45e154c80f3d570cbd02f011863b5446743803a6

You notice the height of the block in the first column. The height is just a fancy way of saying the number of the block. The numbering is very straightforward. The first block was number one, the next number two, etc. Bitcoin has been going on since 2009 and there is a new block about every 10 minutes so there are just under half a million blocks by now (in 2017).

In the fifth column you see the age of the blocks. You can tell that they are roughly 10 minutes apart but not strictly so.
In the last column you can see the hash of the blocks. Notice that the hashes are hexadecimal numbers, notice that they all have the same length and notice how they all have leading zeroes. It is okay for them to have more leading zeroes than required.

If I click on a specific block then I will see more information.



Home / Block - 000000000000000000b012b1eda22dfbd9098ff8ebf76cd62bc60cdb9b37c9af

Summary

Height	494,596	Version	0x20000000	Block Hash	000000000000000000b012b1eda22dfbd9098ff8ebf76cd62bc60cdb9b37c9af
Confirmations	1	Difficulty	1.60 T / 1.36 T	Prev Block	000000000000000000455758fd6b47b0ce0c5d23acab2fd472eb627443f3d3e6
Size	1,034,135 Bytes	Bits	0x1800ce4b	Next Block	N/A
Stripped Size	986,276 Bytes	Nonce	0x674044f1	Merkle Root	93fbba94cb2ac6232730cb6a5fe5af3c278d4324e10a46245b4ae7686e3a87ee
Weight	3,992,963 Bytes	Relayed By	BTC.TOP		
Tx Count	2,143	Time	2017-11-16 09:20:57		

Transactions

Sort: Tx block id Tx hash Fee Sigops Size Weight Inputs count Inputs value Outputs count Outputs value Witness hash

00af416483a43fb4489dc888a7593fd0192ffa29b8b80ad64403846028c6e11b 1.95748384 BTC 2017-11-16 09:20:57

Coinbase

1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ 14.45748384
SegWit commitment output 0.00000000

14.45748384

315edd1ad41d6df382b1f7a7c311431a1d55ee49da596a11419a0b0d2f8fcb48 2,034 Satoshis/byte 0.01662000 BTC 2017-11-16 09:20:57

16J6hr2fVNtmiazc1cyi8EmGRzSgDgp7LP 1.21281056
18sjtANgNb21Lr26bQ8YHcK3UuWiaZd17t 0.00771870
1MciWFDCND4V3KcHxoaEHSqV4HZYcegp4P 0.05286000

1DoEzZDfuWsMxw4zXYkAYa4kLWvbuyyBLA 17.54364803
1GHyAHgzAtrgX2uE75oTzgy88Nq79VfAod 0.01003255

Here I see miscellaneous information like the number of transactions in the block (2,143). Notice how I am also told the hash of the previous block as this needs to be included in the current block. I am also told the nonce for that block.

If I scroll down then I get to see the actual transactions inside the block. In the first column I should see the sender of the coins. This column is given the name “coinbase”. The first transaction represents the reward given to the miner of the block. These coins come out of thin air so there is nothing in the first column except for the word “coinbase”. The amount equals the reward (12.5) plus the transaction fees. Here a total of 14.45748384 bitcoins.

So now why is bitcoin worth anything?

We are used to the idea of gold being worth something. Why was gold so important as an exchange of value throughout history?

Well gold is neither too abundant nor too rare to be useful as a currency. You can't just expect to pick it of the ground like you would sand but there is still enough of it around for it to be of practical use.

Gold is durable. It doesn't rust or spoil. If you have it, you can expect to have it tomorrow.

And finally, this one is really important. It takes work to get gold. It has to be dug out the ground and then processed and purified to make it into a gold coin. Gold represents done labour. It's an act of goodwill between two people. I give you gold that took time and effort to produce and in exchange you give me food or some product that took you effort to acquire.

Bitcoin has many of the same properties.
There are neither too few nor too many of them around.
It cannot rust or spoil since it's only digital.
It does represent done labour since it took spent electricity and an investment in hardware to acquire.

The way the rules are right now, there will never be more than 21 million bitcoins. This might not sound like much but it is possible to spend 100 millionth of a bitcoin. As bitcoin increases in value, smaller and smaller fractions will be used.

	Gold	Bitcoin
Limited supply	✓	✓
Durable	✓	✓
Requires effort to acquire	✓	✓

Cold storage

Imagine you have a box with a lock. You want people to use the box to send you stuff but you don't want thieves to be able to open the box. You give people a public key. It can be used to close the box but once closed the same key won't open it. You keep a private key and that's the only key that can open the box. It takes a public key to close it but a private key to open it.

This is widely known as public-key cryptography and is ubiquitous in our modern world. When you communicate with your bank over the internet, the bank sends you a public key. The key is used to encrypt the information you send them and only the bank can decrypt it with their private key. All this happens in the background without you necessarily being aware of what's going on.
In many browsers this is represented by a green padlock in the top left corner to let you know that the communication is encrypted.

With bitcoin, a public key enables people to send bitcoin to your wallet. Your private key is the only way to have access to those bitcoins. Most people use websites that offer bitcoin wallets and shield them from the technical details required. A username and password gives access to the bitcoin in their wallet and the private keys are managed by the website.

When private keys are managed by third parties online, there's always a chance that a hacker will steal the bitcoins. The safest but also least convenient way of storing bitcoin is by means of cold storage. In that situation the private key is taken off the internet and any computer and instead written or printed on a piece of paper and kept in a safe.

Cold storage is used for secure long term storage. It is good practice for companies that manage bitcoin for customers to keep at least a fraction of their reserve in cold storage in order to mitigate risks.

> Cold storage is the offline storage of the private key to a bitcoin wallet for more secure and typically long term storage.

Is bitcoin anonymous?

Bitcoin is completely anonymous as long as you stay strictly within the bitcoin system. When creating a bitcoin wallet there is no requirement to give your name or address. You can go to bitaddress.org and generate a new bitcoin wallet completely anonymously. You are then responsible for managing this wallet and keeping the private key safe. People typically don't do this however and choose the convenience of various websites that offer an easy interface to use bitcoin. Those websites require varying degrees of identification before they may be used.

There are a couple of ways that your transactions may not be anonymous. The obvious one is when you tell people what your bitcoin address is. People can then look up your wallet in the blockchain and follow your transactions both forwards and backwards in time. To mitigate this, some businesses give every customer a new bitcoin wallet for every transaction.

Another way is when you use exchanges; these are places where you can buy and sell bitcoins for other currencies. Depending on where in the world they operate, they may be subject to a wide variety of different legislation. Exchanges typically require that you identify yourself and require varying degrees of proof.

Some will argue that honest people have nothing to hide while others will argue that governments cannot be trusted and thus shouldn't know their business.

> While it is possible to be strictly anonymous with bitcoin this is typically not the case unless one does take precautions.
>
> Do note however that once specific bitcoins have been identified in the blockchain, they are completely traceable both forwards and backwards in time.

Cryptocurrencies: security and future innovations

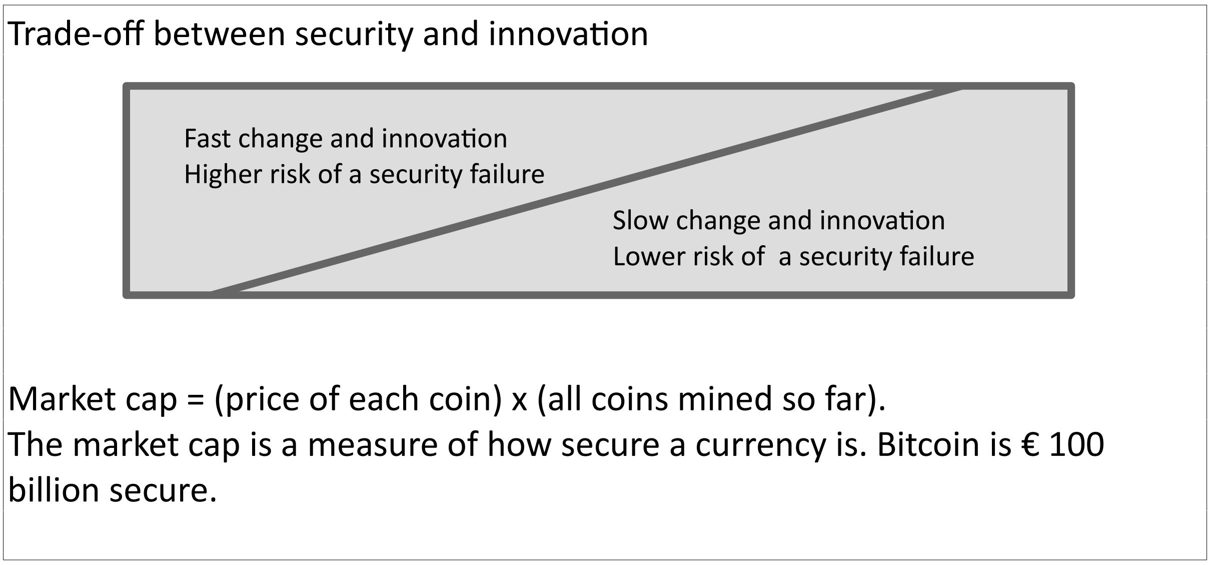
Bitcoin is only one of many different cryptocurrencies. A cryptocurrency can loosely be defined as a system that uses a blockchain to exchange value between parties.
One needs to realize that there is a bit of tension within the community of cryptocurrencies. Some criticize bitcoin for falling behind when it comes to the technology. Changes to bitcoin tend to be slow and small. Bitcoin is rather conservative.
Other cryptocurrencies want to innovate and push the envelope and evolve a lot faster. With this faster change comes some risks. The faster a technology does change, the higher the risk flaws being introduced and being exploited by hackers.

Ethereum is an example of another such cryptocurrency. It wants to innovate and is less conservative than bitcoin. A hack caused coins to be stolen during ethereum's history. A part of the community wanted to roll back the changes so people could get their money back, others wanted to continue with the existing blockchain without rolling back anything. This is the reason why today we have ethereum and ethereum classic.

So far the bitcoin protocol has never failed and never been hacked. If you hear stories about bitcoins lost or stolen then this is usually the result of people's negligence. If you hear of accounts being hacked then this is the fault of third parties that manage bitcoin wallets for you. Mt gox is a famous such example. It was a company that managed people's bitcoin but their security was breached and a lot of bitcoins got stolen.

Today (November 2017) a bitcoin is just over € 6,000. The total number of bitcoins mined so far is 16.6 million. That means that all the bitcoins together are worth roughly € 100 billion. This is known as the "market capitalization" or "market cap" for short. The higher the market cap, the bigger a target a cryptocurrency becomes for criminals and hackers. If the currency were hacked then the value of individual coins would drop and so would the market cap. Thus, we can think of the market cap as a measure of the reliability and security of the cryptocurrency. Right now, bitcoin is € 100 billion secure.

The website https://www.coinmarketcap.com does list the market cap for many different cryptocurrencies.



Trade-off between security and innovation

Fast change and innovation
Higher risk of a security failure

Slow change and innovation
Lower risk of a security failure

Market cap = (price of each coin) x (all coins mined so far).
The market cap is a measure of how secure a currency is. Bitcoin is € 100 billion secure.

21 million and no more?

Once 21 million bitcoin will have been mined, no more bitcoins will ever be mined. Miners will need to rely strictly on transaction fees as an incentive to mine. At least, that's the theory and that's how the rules are right now. There are two things to consider here though.

The first thing is what I call "dead bitcoins". These are bitcoins where the owner has either lost their private key or they died and didn't pass it on to anyone. Dead bitcoins are bitcoins that for some reason or another are no longer accessible. They are still technically in the blockchain but no longer in circulation. As time goes on, more and more bitcoins will be dead.
Dead bitcoins cause deflation. Since fewer bitcoins are in circulation, the value of each bitcoin goes up. As the value goes up, smaller and smaller fractions of a bitcoin will be spent. The smallest fraction of a bitcoin that can be spent is one hundred millionth of a bitcoin. This is called a Satoshi in honour of the inventor of bitcoin. As more bitcoins become dead, the value of Satoshis will go up. Right now, the value of a Satoshi is negligible and that's the way you want it. If the value goes up too much, how will you pay for small things? It will take a really long time before any of this becomes a problem but as the value of a Satoshi becomes too high, there will be a need to lower the value of bitcoin by producing more bitcoins. The idea of 'never' raising the cap is not sustainable.

The second thing will become a problem much sooner. It relates to the queue transactions go into. Before transactions find their way into a block, they go into the "mempool". Transactions are not placed in the blocks in the order in which they were generated but based on their fee. So, if you want to see a transaction confirmed quickly, you need to volunteer a high fee.
What will happen when the rewards become very small? Mining bitcoin will become less profitable and thus miners will drop out. This is bad news as it makes bitcoin less decentralized and therefore less stable. The solution to miners dropping out? Either raise the fees or raise the cap!

Will raising the cap cause inflation and decrease the value of bitcoins? If the rate at which bitcoins are generated is equivalent to the rate at which bitcoins become dead, the value will remain stable.
How realistic is the raising of the cap? Raising the cap would require 95% agreement among the miners. Of course, it's precisely those miners that have the incentive to raise the cap as the mining becomes less profitable so I believe it is reasonable even inevitable, given enough time, that the cap will be raised.

Hope you enjoyed!

If you found this information helpful then maybe you would consider a donation.

bitcoin:
1EKMkZi3m5f79fZxnx4nEyDfjuPv57h8km

litecoin:
Lh3wU6gZDeHGA5uEXvFkH1YXHErxVr8MkH

Ethereum:
0xbAa0C7312053Ea1918B62dAe9da6e9D6F61BAD6a

Alternatively, you may also do a fiat donation through paypal:

greggink@gmail.com