Bitcoin explainer for beginners

Who invented it and why?

Bitcoin was originally described in January 2009 by an anonymous creator called Satoshi Nakamoto in a white paper before being released as a free software project. It was invented in response to the 2008 financial crises where governments spent hundreds of billions to bail out banks and pump money into the markets. This has an inflationary effect, Bitcoin is designed to be deflationary with less issued over time (see fig. 1). There is no money printing in times of crisis and no bailouts. Instead Bitcoins are generated in a controlled way determined by an algorithm. That it’s free software means anyone can study and contribute to the code. This helps ensure that not just one entity has control over it and a community can be fostered around it to develop and maintain it.

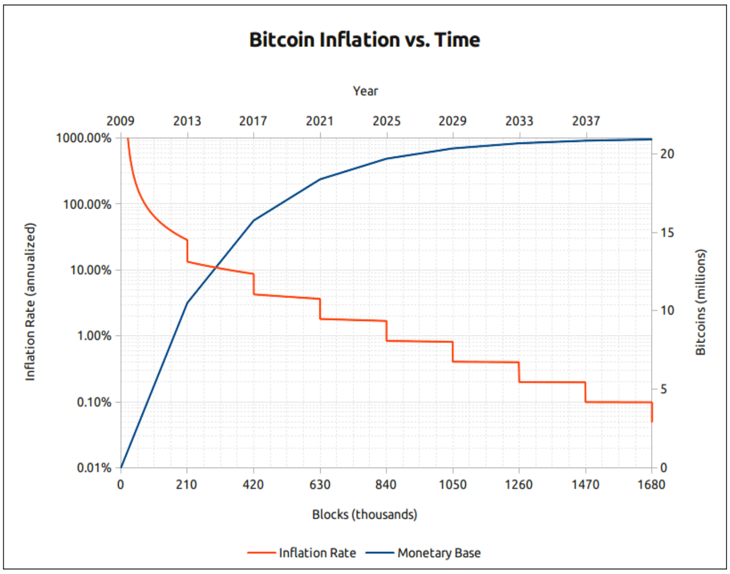

Figure 1: Less Bitcoin is issued over time making it deflationary

What is it and what makes it so special?

Bitcoin is best thought of as digital gold. It requires no banks or governments and cannot be manipulated by governments. For the first time there is a currency that’s recognised as having value all over the world. You have full control but also full responsibility for your money. It has been a life line for people in countries like Venezuela where the local currency has lost its value. In these cases Bitcoin can act as a store of value.

Money can be sent between any 2 individuals anywhere for a low transaction fee or free, near instantly as long as they have a computer or phone with an Internet connection. There are no banks or other third parties such as card companies required and transactions are secured by the work of the miners using strong cryptography.

There had been several other attempts at creating an e-cash before Bitcoin but they had all failed. Bitcoin solves the problems all of them had by combining well understood technologies in a new and innovative way.

Wallets

A wallet is required to store Bitcoins. This can be done using an app which will usually prompt you for a password, or a hardware device which is more secure.

Each wallet has a unique ID. You send and receive Bitcoins through your wallet software. It will also tell you what they are worth at the current market rates and include features to make it safer and easier to transact e.g. by allowing you to scan QR codes to get a recipients wallet address instead of having to copy and paste it.

> *"The root problem with conventional currencies is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."*
>
> \- Satoshi Nakamoto in the Bitcoin whitepaper

Wallet recovery

When you make your wallet initially it will give you 12 recovery words. These should be carefully and securely stored as they will allow you to reconstruct the cryptographic keys which secure your wallet and perform transactions again in case of any issues. If you lose your password and recovery words you have lost access to your Bitcoin.

That’s great but how do I get some?

You can either mine one which now takes a lot of computing power (often referred to as hashing power) in the form of specialised hardware to be economical, or you can buy one from an online exchange as you might use a currency exchange to buy holiday money. You should then transfer it to your own wallet. Exchanges represent big, juicy targets to hackers and have been compromised and gone out of business in the past. A notable example being Mt Gox in 2014.

How do I know I can trust the exchange?

Any reputable exchange will require you send proof of ID-whether buying or selling to comply with KYC (Know Your Customer) AML (Anti Money Laundering) rules.

When you do a transaction the seller must first deposit the Bitcoin in a wallet on the exchange. The exchange holds these in escrow until the seller has confirmed that the buyer has paid. Only then are the Bitcoins released to the buyer. As this is a wallet you don’t control, it’s good practise to move them off the exchange once you have them.

Price volatility

While the price remains volatile Bitcoin is not subject to supply shocks as with precious metals and other commodities where the value can suddenly be greatly reduced when new deposits are found. As more Bitcoin has been issued volatility has greatly reduced.

Miners and rewards
Miners are crucial to the supply of Bitcoins and the security of the system and so are incentivised to do their work by being rewarded with Bitcoins and transaction fees.

As gold requires time and effort to mine out the ground, Bitcoins require time and effort to be performed before they are issued. Bitcoin is therefore ‘backed’ by a proof of work and have a value represented by the electricity and hardware required to mine them.

When Bitcoin first started miners were rewarded with 50 Bitcoins when they processed a block. The first block is known as the Genesis block and is a special case and is unspendable.
After every 210,000 blocks (approx. every 4 years) the number of Bitcoins miners get rewarded with halves in an event known as the halving. Some think these events help drive cycles in the price. All Bitcoins that will ever exist will have been generated by around 2140.

The block chain
Every time a transaction is made with Bitcoin (someone spends it or transfers it) the details get broadcast to all nodes on the network who bundle transactions (sometimes abbreviated to Tx) into a block. Blocks ideally consist of the last 10 minutes of transactions. Each node or ‘miner’ then processes the block for a reward. The start of each block references the last hash in the one before it creating a blockchain. The nodes miners run contain a copy of the full blockchain with every transaction ever made on it. Every Bitcoin transaction is therefore in a public distributed ledger. Every transaction must be public so miners can be sure that the same coin hasn’t been spent twice.

Transaction fees
When you send Bitcoin your wallet software will usually include a small fee which gets included in the block. Miners favour blocks which include such tips. These blocks therefore get processed faster. While transaction fees are optional it will become more significant as the Bitcoin reward for miners decreases and they become more reliant on transaction fees.

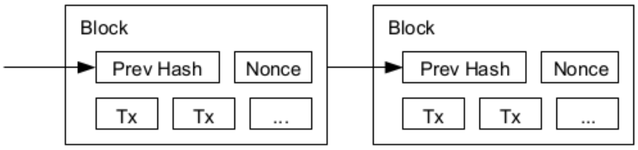

Figure 2: The structure of the blockchain

What’s a hash?
A hash is an algorithm that takes some data, processes it and outputs an identifier of a fixed length that is unique to the input data. Changing even one part of the input will give a different hash. The hash Bitcoin uses is called SHA-256 which a widely used standard. These are used every time Bitcoin is transferred.

Mining difficulty – how the supply of Bitcoin is regulated
As the processing power of the miners rises and falls the difficulty of the work demanded of them is adjusted to ensure that Bitcoins are being issued at a consistent rate. The miners must find a valid cryptographic hash for the block which begins with a set number of zeros. The number of zeros required at the start of the hash is determined by the difficulty. The rate at which they can compute hashes (often referred to as solving mathematical puzzles) is known as their hashing power.

Units
Bitcoins are divisible to 8 decimal places with the smallest unit called a Satoshi after it’s creator. This works out to be 2.1 quadrillion monetary units of currency (Satoshi) or just under 21 million Bitcoins. There are approx 7.6bn people alive today so there are 2,763,157.89 Satoshis for each person alive today.

Changes to Bitcoin
Some free software projects such as Linux have a leader (often the person who first developed it). As Bitcoin has no one central leader, decisions are made by consensus among the community.
Since it was invented there have been numerous improvements made to how it works. These are referenced by their corresponding BIP numbers (Bitcoin Improvement Proposals). They are usually discussed among the community first, then submitted as drafts with sample code. They are then scrutinised and refined. If the proposal reaches community consensus, it will be considered final. They are finally adopted when developers implement them in code. Implementations of changes are then coordinated among the miners so that they are all adhere to a consistent set of rules.

The Lightning network
Bitcoin can process only 7 transactions per second and can take several minutes or more (dependent on the transaction fee) to verify a transaction. When using the lightning network you setup a payment channel with a person or place you send money to regularly. Instead of making a transaction on the block chain each time, you set an amount aside and a record is kept of each transaction. Like pre-paying a bar tab, you can only spend as much as you’ve put behind the bar and either party can settle the bill at any point (but both must agree to do so). It is only the sum amount that is released by miners when this happens.

Because you can have lots of transactions in this way and you’re not paying fees to miners each time it’s a much faster and cheaper way of using Bitcoin.

> *The one thing that's missing, but that will soon be developed is a reliable e-cash. A method whereby on the internet you can transfer funds from A to B, without A knowing B or B knowing A. The way in which I can take a twenty-dollar bill and hand it over to you, and there's no record of where it came from and you may get that without knowing who I am.*
>
> - Economist Milton Friedman predicting the invention of a Bitcoin like e-cash in 1999