Tell Me about Bitcoin

What is Bitcoin?

Bitcoin is a protocol for exchanging value, from one peer to another, over an electronic communications network. Unlike traditional online payment solutions and services (PayPal, Venmo, automated clearing house (ACH) transfers, bank wire transfer, etc.), Bitcoin does not rely on a trusted third party to perform transactions; it is purely "peer-to-peer."[1]

Okay that's great, but what is it really? How does it work?

The best description that I have found is a YouTube video on the channel 3Blue1Brown. Here is the link: https://youtu.be/bBC-nXj3Ng4. It is 26 minutes long but it really does fully and accurately explain, *exactly*, what Bitcoin is, and it's also quite entertaining. Friends of mine have reported that it is a very helpful video.

Who created it?

Bitcoin was created by the pseudonymous person, or persons, named Satoshi Nakamoto.

Why was it created?

It is generally believed that the motivations for Bitcoin's creation were: 1) the inherent flaws in traditional financial systems, and 2) the dishonest and fraudulent behavior—made possible by such inherent flaws—of traditional financial institutions. To quote Nakamoto,

> "The root problem with conventional currency 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. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts."[2]

Why should I buy it?

There are numerous reasons to buy Bitcoin. One reason that most people find compelling is that the value of Bitcoin has appreciated extremely quickly, and continues to appreciate faster than every other asset class. The caveat, of course, is that the price is extremely volatile. Given enough time, however, the value of Bitcoin eventually rises above the value at which it was purchased, and when it does, watch out! The enormous gains seen in Bitcoin are unlike anything you'll find in traditional assets. If you're lucky, buying and holding a diversified portfolio of stocks, bonds, real estate, commodities, and precious metals will get you an average annual return of about 7-15%, give or take. A buy-and-hold investment in Bitcoin, on the other hand, has provided an average annualized return greater than 100% during the past 5 years, and an annualized return of greater than 1000% during the past 10 years. Many bullish investors believe, very strongly, that this trend will continue for many years.

An even more compelling reason to buy Bitcoin, though, is more subtle, but it may very well become obvious in the years to come: *not* buying Bitcoin, or waiting too long to buy Bitcoin, might actually be detrimental to one's finances. This is especially true as more and more people adopt Bitcoin as a store of value and/or medium of exchange. Many have described this as a game of musical chairs[3] [4] [5] [6] because the total number of bitcoins that will (or can) ever exist is 21 million, and 18.5 million are already accounted for. As central banks around the world increase the total supply of fiat currency by the tens of trillions, and meanwhile Bitcoin becomes scarcer and scarcer, Bitcoin might become increasingly difficult, and financially painful, to ignore.

Why does the price go up so fast?

Prices of all tradable securities are ultimately determined by supply and demand. This explains why the price of the futures contracts on oil actually went *negative* in April 2020[7]; if there's a steady supply of oil being delivered and nobody wants to buy the oil because everybody stopped traveling due to a global pandemic, then you actually have to pay people to take the oil. But, if the opposite is true—very little supply and an enormous demand—then the price goes parabolic, and can increase by many multiples. Bitcoin was designed such that the steady flow of newly "minted" bitcoins is cut in half every 4 years, but the demand continues to increase because the price keeps going up. This creates a positive feedback loop that is unique to Bitcoin: supply rate is cut in half -> price goes up -> demand goes up -> price goes up -> demand goes up. This positive feedback loop was the reason why the price of Bitcoin went from $800 in December 2016, to $20,000 just one year later.

An important bit of research was published by a Dutch analyst in March of 2019 that explains, quantitatively, how the scarcity of Bitcoin is related to its price[8]. The paper is not an academic article that requires a PhD to understand, but it does have a little bit of high school math: https://tinyurl.com/btc-cycle.

What about all the other cryptocurrencies?

The existence of other cryptocurrencies besides Bitcoin has been compared to the variety that exists in metals—gold is the most valuable and is the best store of value, and there exists other metals such as silver, platinum, iron, copper, etc. In the same way alchemists will never be able to turn iron into gold, it is impossible to make a Bitcoin from an Ether token, or from a Litecoin. Yes, they can be traded for one another, but the reality that underlies all cryptocurrencies is the network of people who run their respective protocol software. As written at the top of this page, Bitcoin is a *protocol* that is followed by a network of people who run the protocol's software to either "mine" for new units, or to validate transactions and thus reach consensus on the current state of the blockchain. As of this writing, Bitcoin is, by far, the most decentralized, the most powerful, and therefore the most secure network in existence. (This includes other networks besides cryptocurrency—even in April of 2015, when the hashpower of the Bitcoin network was over 400 times *less* than it is currently in the year 2020, Bitcoin's hashpower was over 100 times greater than the

[1] https://bitcoin.org/bitcoin.pdf
[2] https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/
[3] https://www.cityam.com/bitcoin-is-a-game-of-musical-chairs-and-the-music-is-stopping/
[4] https://medium.com/@AJC241469/the-game-of-musical-chairs-that-were-all-playing-4af3e4234d5e
[5] https://bankless.substack.com/p/bitcoins-scarcity-game
[6] https://cointelegraph.com/news/middle-eastern-restaurant-chain-converts-entire-reserves-to-btc
[7] https://globalriskinsights.com/2020/05/making-history-coronavirus-and-negative-oil-prices/
[8] https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

hashpower that could be achieved using all of Google's datacenters. So, for the purpose of securing a blockchain by hashing power, the Bitcoin network is currently on the order of 10,000 times more powerful than all of Google's datacenters *combined*[*].)

But…

… a whole Bitcoin is so expensive, I can't afford it!

Just like one US dollar is divisible into 100 cents, one bitcoin is divisible into 0.00000001 bitcoin. This is the smallest piece of a bitcoin that can be owned, and it was named after Bitcoin's creator; it's called the satoshi, often abbreviated to just "sat." 1 sat = 0.00000001 bitcoin. Equivalently, 100,000,000 sats = 1 bitcoin.

… the price of Bitcoin is so volatile!

Yes, it is. Bitcoin is relatively new, and its total value is orders of magnitude less than the value of existing fiat currencies. Its total value is also likely to be orders of magnitude less than what its future value will be. It is practically impossible for an asset to go from a total value in the millions of dollars to the trillions of dollars without a lot of big ups and downs. But, it's okay; a strategy that most people find effective is to dollar-cost-average their purchase of bitcoin. That is, they buy small amounts, regularly, over a long time span. This way, if the price happens to go down 10% or 20% just days after your initial purchase, there's no need to sweat because you only bought a small amount, and you'll be buying more at the lower price. This strategy effectively reduces the perception of volatility that your wallet would otherwise feel if you bought a large amount all at once.

… governments will ban it!

This was a major concern during the initial years of Bitcoin's existence. Recently, however, that threat has almost completely abated for two reasons, 1) such a ban would now be very impotent due to the rapid expansion and decentralization of the bitcoin network around the globe, and 2) legislation and legal precedents are starting to create a legal foundation for Bitcoin's persistence, and for individuals to own Bitcoin. A recent episode on The Investor's Podcast Network sheds more light on this topic: https://tinyurl.com/btc-legal.

… there might be a fatal flaw in the code and then all my money is gone!

The blockchain architecture ensures that all bitcoin funds are recorded identically on thousands of computers (nodes) around the world. This is one of the reasons why Bitcoin is actually extremely secure; the only way your Bitcoin funds could be altered, other than using the private keys to perform a transaction, would be to destroy every copy of the blockchain… simultaneously. If not simultaneously, then one would have to shut down the entire global internet, and then destroy every copy of the blockchain, one by one, before the internet could be restored. The point is, once a transaction is recorded into the blockchain, it is practically impossible to change. FYI, there are Bitcoin nodes storing the entire blockchain in over 100 countries, and there is even a Bitcoin node on a satellite in space!

… Bitcoin has no intrinsic value! It isn't backed by anything!

The truth is that there is no such thing as intrinsic value. What we call "value" is merely a quality that is ascribed to things by human beings. As von Mises wrote,

> "Value is the importance that acting man attaches to ultimate ends. Only to ultimate ends is primary and original value assigned. Means are valued derivatively according to their serviceableness in contributing to the attainment of ultimate ends. Their valuation is derived from the valuation of the respective ends. They are important for man only as far as they make it possible for him to attain some ends. Value is not intrinsic, it is not in things. It is within us; it is the way in which man reacts to the conditions of his environment."[9]

… [insert objection here]!

Ultimately, you and you alone are responsible for your finances. Many objections can be raised, but at some point one must recognize the reality of the current situation: technologically advanced civilizations of the world are using a broken and blatantly unfair financial system that provides a huge advantage to those who are already rich and powerful. If you think that's mere conspiracy then it's suggested that you do yourself a favor and Google search *The Cantillon Effect*. It's so obvious that a child could figure it out—just try playing a game of Monopoly with some children and bring a printer with you to print new Monopoly bills in case you start to lose; they'll point out your cheating ways very quickly. Sometimes it really does take a child to realize the Emperor has no clothes.

In a modern society, whether it is governed as a Democracy or a Constitutional Republic, there should not be a group of individuals who can create money from nothing while almost everybody else has to work their entire lives just to survive. The enormous wealth inequality of the 21st century is not a result of capitalism, socialism, or political corruption, but rather a result of incredibly unfair financial chicanery from the banks. Bitcoin is an open protocol that gives financial sovereignty back to the people—they only need to claim it.

Where can I learn more?

https://www.lopp.net/bitcoin-information.html

[9] https://cdn.mises.org/Human%20Action_3.pdf, pg 96.

* Technically, this is mostly due to the fact that the Bitcoin network is secured by special hardware called Application Specific Integrated Circuits, or ASICs. Unlike the CPUs in Google's servers, ASICs are designed to perform one function: hashing.