

understanding bitcoin

How it all started

Shortly after the 2008 engineered "financial crisis", which should actually be called "the biggest heist in history", someone under the pseudonym of [Satoshi Nakamoto](#) released a white paper introducing the Bitcoin concept. In 2009 he released the free and open source [Bitcoin software](#) which started the network and mined the first units called Bitcoins (BTC).



At that time, Bitcoin was a whole new concept and only a few people were actually aware of it and started mining it. Back then, bitcoins were extremely cheap - you could only buy a [pizza for 10,000 BTC](#).

I first heard about Bitcoin in early 2012 but did not take it too seriously until later that year, when I saw the news about the Iranian people [bypassing](#) the US-imposed sanctions by using Bitcoins as a means of money transfer. That got my attention.

How does Bitcoin work?

Bitcoin does not have a central authority, there is no bank of Bitcoin, CEO of Bitcoin or any other centralized "authority" service. Bitcoin is powered by its network nodes, the matrix of world-wide computational devices interconnected, based on the peer-to-peer (p2p) protocol.



This means Bitcoin cannot be shutdown by anybody, there is no kill switch, there is no head of the snake that can be cut off, there is no way any government on this planet could possibly shut down Bitcoin, because it's been designed in such a way to be immune to corporate or private control.

All Bitcoin transactions are stored in a public ledger called [blockchain](#). This is accessible to everybody for free and every single transaction that ever took place is being archived there forever and can be viewed by anyone, along with an entire thread of related transactions. No names are being associated with them, since you don't need your personal details to create Bitcoin transactions, except if you exchange them to fiat, that's where the online exchanges require user verification.

There are a few notable online exchanges that allow purchasing bitcoins with fiat money. [Bitstamp](#) is probably the best of all. Some of the exchanges have been attacked by hackers and had their bitcoins stolen. It's truly a Wild West of cryptocurrencies out there so it's highly recommended that you do your homework before getting involved with Bitcoin.

The number of Bitcoins that will ever be released is 21 million. There will never be anything more than that. Half of that amount is already in circulation and the other half will be mined by the end of 2140, which means it's getting increasingly more difficult to produce bitcoins, giving it greater value over time.

[Mining](#) is the process of creating bitcoins, just like you would mine for gold or diamonds, but instead of exploiting nations to slave their lives into digging for precious metals, bitcoins only require computational power, which means you can mine them using your computer. Initially, that used to work but now the mining difficulty has increased to such a degree, that it requires specialized and expensive mining rigs using [ASIC](#) hardware.

Bitcoin can never be printed out of thin air, like the [FED](#) does in US. Bitcoin does not care about gold, and that's great because many countries rich in gold resources are being exploited and people are forced to live in poverty, so just because a country has gold resources, its people are not guaranteed a high standard of living. And what about other countries that don't have gold? Should they be poor for all eternity?

Here's a scenario

You're working overseas and want to send money back to your family who live across the other side of the globe. Your options are limited: use a bank transfer or money transfer services like MoneyGram or Western Union. These services are time consuming, have extremely expensive fees and take a few working days to clear out + weekends. With Bitcoin, you need just two wallets and one specific address. Wallet A is yours and you input the amount you want to send to the address of wallet B.



Distance is irrelevant. It does not matter which country wallet B is in, or if it's Weekend, day or night, holiday, nothing like that matters. Once you hit the Send button, an extremely small (and fixed) fee is being subtracted from your fund (only a few cents) and the rest goes straight to wallet B, in a matter a few minutes and will take an overall of 10 minutes to get validated by the network and clear out to wallet B. That's it. It doesn't matter if you send the equivalent of 1 dollar or 1 billion dollars. The fee is always the same (0.001BTC). Some work is being done to lower that fee, since the price of BTC might increase over time and the fee should not grow with it.

Another advantage of Bitcoin is that it can't be blocked by Paypal, Visa or MasterCard or any other financial institution, like it happened with WikiLeaks when their funds got **frozen** and people could not donate money to them. But now they accept bitcoins and nobody can interfere with that.

How to get started with Bitcoin?

At the time of writing this, the safest way to get Bitcoins is to register with an online exchange, have your identity verified with them, deposit fiat money into their account via bank transfer (online transfer) and then start buying bitcoins. There are many online exchanges available, but most of them have either been hacked, or closed down, or just experience many technical problems. I recommend using bitstamp.net. It works great for Europeans but also accepts international transfers. It's the biggest (and actually the best) online Bitcoin exchange. It used to be second after the **defunct MtGox**, but has now taken the throne.



Do some research on forums about any online exchange that you choose and try not to send large amounts at first, just play with it, test it out. The best way to save your bitcoins is by using **desktop wallets**, but this is also a risky option, since computers can be hacked, there are viruses and malware, you can accidentally delete you wallets, and so on. More about securing your computer [here](#).

You can keep your bitcoins in desktop wallets, online wallets or even cold storage online **vaults**. Apple is currently **blocking mobile wallets**, but they work on Android devices. A more technical explanation can be found in [this video](#).

Bitcoin moving forward

I think it's pretty obvious that Bitcoin is getting more media attention and a growing number of Bitcoin-related services are emerging on a daily basis. There is still opposition on the part of some governments, but I see no way of completely dismantling Bitcoin. This is a whole new technological framework which is not limited to Bitcoin itself and can provide support for many new applications and services many of whom are already in the making. **Ethereum** is one example.



Any opportunity to smear Bitcoin with negative news has been - and is still being used. China initially embraced Bitcoin, but later turned against it, but it's still in the midst of making up their minds. Russia has been rumored to unofficially ban Bitcoin, while the rest of the planet has embraced it, many BTC ATM machines are being deployed world wide, you can buy products and services with Bitcoin, overstock.com accepts BTC payments and the whole adoption process is growing exponentially.



MtGox saga

If you've been around the crypto-world for a while, you're probably familiar with the status of the Japanese online exchange [MtGox](#). For a while, it was by far the biggest Bitcoin online exchange in the world, handling more than 70% of all the bitcoins transactions.

However, it experienced many technical problems and ended up losing most of people's money (approx. 750,000 BTC) and had to eventually file for bankruptcy and liquidation. They managed to later [find 200,000 BTC](#) in an old wallet, but they were still short of approx. 550,000 BTC.

There were rumors about Bitcoin crashing due to MtGox status, as if this would all be a Ponzi scheme, but if you look carefully, not only that did not happen, but it can't happen.

You can build a company which could be used as a Ponzi scheme, but that has nothing to do with Bitcoin itself. A similar example would be with a normal bank. If the bank goes bust, people might lose their money and the government might need to cover that, but it doesn't mean the fiat currency was a Ponzi scheme, it only means that a big bank went bust. Bitcoin has no owner or central authority, there is no such thing as a bank of Bitcoin. MtGox Wikipedia full article [here](#). [Bitstamp](#) is now the world's [largest](#) online exchange.

Wrap-up

If it's something you need to let sink in, is that we're already in a new financial era, we already have a way to store, exchange and spend our currency, completely independent of all natural resources, banks or other financial entities. This is a glimpse of what it actually feels like to be free. The resistance battle is still going on and the worse has yet to come, but one thing is for sure: Bitcoin is here to stay.

Some conspiracy theorists point out that Bitcoin is the "mark of the beast", the "one-world-government-currency" or a giant Ponzi scheme, but they don't provide any clear and logical arguments for that, just fear mongering. The more you study how Bitcoin works and understand it, the more you realize it's actually the people's currency, a new and improved way of financial freedom and independence, a complete paradigm shift.

Best website I found for keeping up-to-date with Bitcoin news is [CoinDesk](#).