



Bitcoin Explained In Simple Terms

by iBek Esengulov

Foreword

Crypto newcomers have a mountain of questions. What is Bitcoin? Why should you care about crypto? What makes Bitcoin so unique? How does it work? And how can you invest?

The purpose of this guide is to answer those questions by introducing you to Bitcoin and other cryptocurrencies in simple terms and an easy-to-digest manner.

This guide was written for someone who has little to no technical knowledge about Bitcoin, crypto, or blockchains.

To aid accessibility, some of the technical concepts have been simplified to make it easier for a non-technical person to grasp the essential information.

Table of Contents

About Bitcoin	4
Where Did Bitcoin Come From?	4
How Does Bitcoin Work?	5
Bitcoin by the Numbers	7
Bitcoin Forks and Other Important Cryptocurrencies	8
Why Bitcoin	10
From Idea to Reality	10
Why Is Bitcoin Growing?	11
Can the Growth of Bitcoin Be Stopped?	12
Getting Started With Bitcoin	14
How to Buy Bitcoin With a Credit Card	15
How to Buy Bitcoin on an Exchange	15
Storing Bitcoin Safely	17
Bitcoin Wallets Explained	17
Understanding the Private Key	19
Storing Private Keys Securely	20
Recommended Non-Custodial Wallets	21
What Happens If You Lose Your Phone?	21
Using Bitcoin	23
How to Receive Bitcoin	23
How to Send Bitcoin	24
How Fast Are Bitcoin Transactions?	25
Bitcoin Privacy Explained	27
Using Bitcoin for Purchases	28
Bitcoin Nodes and Mining	30
Do You Need to Run a Node?	30
Different Types of Nodes	31
Is it Profitable to Run A Node?	31
Time to Begin Your Bitcoin Journey	32
About the author	33

About Bitcoin

Let's begin by learning a little about Bitcoin's basic principles.

Where Did Bitcoin Come From?

Over the last few years, Bitcoin has been labeled in many different ways. It's been called everything from electronic cash to digital gold.

While Bitcoin's definition may change depending on who you ask, it holds certain universal properties which gives Bitcoin value. Consequently, many people regard it as a better alternative to traditional fiat currencies and other physical assets such as gold or silver.

The idea of Bitcoin was first proposed by Satoshi Nakamoto back in 2008. Satoshi's original whitepaper created a blueprint how to perform decentralized financial transactions. It removed the need for third-party intermediaries such as banks and credit agencies.

The images below demonstrate the difference between a centralized network (i.e. the traditional monetary system) compared to the decentralized Bitcoin network.

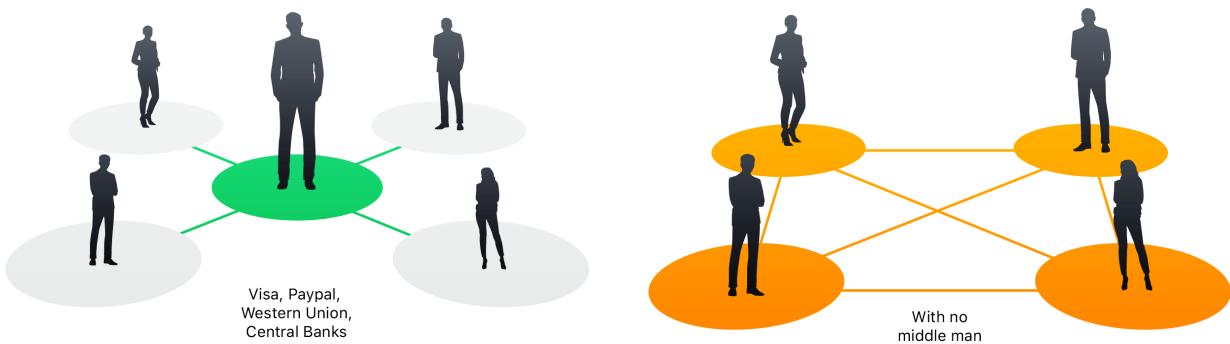


Fig. 1. Centralized network (left) vs decentralized network (right)

In the paper, Satoshi Nakamoto proposed Bitcoin as a decentralized network that is:

- Not reliant upon any central entity to remain online.
- Functional 24 hours a day without dependence on any external entity.

- Has equal rules for all network participants
- Available for anyone to use without conditions.
- Works across geographical borders.

The ideas put forward in the paper required a comprehensive understanding of the contemporary monetary system and graduate-level knowledge of mathematics, cryptography, and computer science. As such, you should regard Bitcoin as a scientific invention that challenges the hegemony of the present-day monetary system and the regulatory entities supporting it.

How Does Bitcoin Work?

Usually, when someone talks about Bitcoin or the Bitcoin blockchain, they are referring to the Bitcoin network.

The image below illustrates the basic structure of the Bitcoin network. There are two types of parties participating in the network: wallets and nodes. Some Bitcoin network nodes are also known as miners.

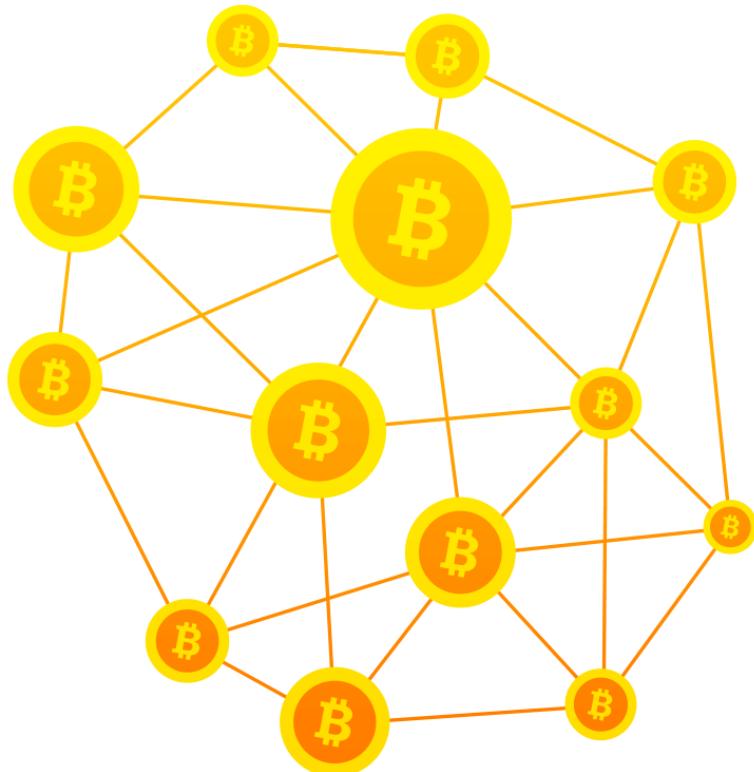


Fig. 2. Basic structure of the Bitcoin network.

Anyone can join the network as a node or as a wallet, then start using with Bitcoin on equal terms with everyone else.

- I. Bitcoin users typically own wallets. They can send and receive payments.
- II. Nodes are the entities which validate Bitcoin transactions and keep a history of transactions. A node can also act as a wallet.

While every network participant is able to send and receive Bitcoin payments, only nodes log the entire history of transactions in real-time. The log of transactions is called the Bitcoin blockchain.

The word blockchain originates from the practice of adding new transactions to the log in chunks (called blocks). The new blocks are added roughly once every 10 minutes.

Nodes are also tasked with validating every new transaction and ensuring that only legitimate transactions are added to the blockchain. Anyone can set up a node without much effort. A node doesn't require any maintenance and can operate autonomously, even on an old computer. It only requires an internet connection to function.

If a node tries to cheat the network by marking an invalid transaction as valid, it would be disregarded by all other nodes on the network. Cumulatively, therefore, nodes guarantee the openness, availability, decentralization, and security of the network. Cheating on such a network is close to impossible.

There are over 10,000 Bitcoin nodes powering the network at any given time. The nodes are spread around the world.

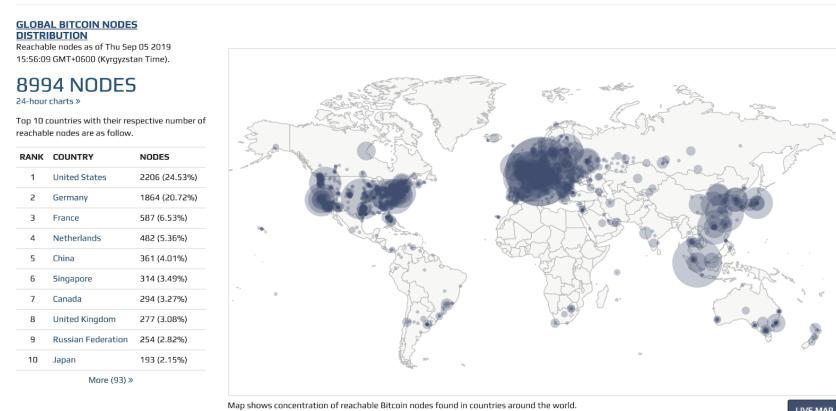


Fig. 3. Global Bitcoin nodes distribution.

Anyone can set up a Bitcoin node at home and act as one of the guardians of the Bitcoin network. We'll take a closer look later in the guide.

Bitcoin by the Numbers

Eventually, there will be 21 million Bitcoins in existence. So far, almost 18 million Bitcoins have been released to the market. The Bitcoin network will create the remaining three million over the next 130 years.

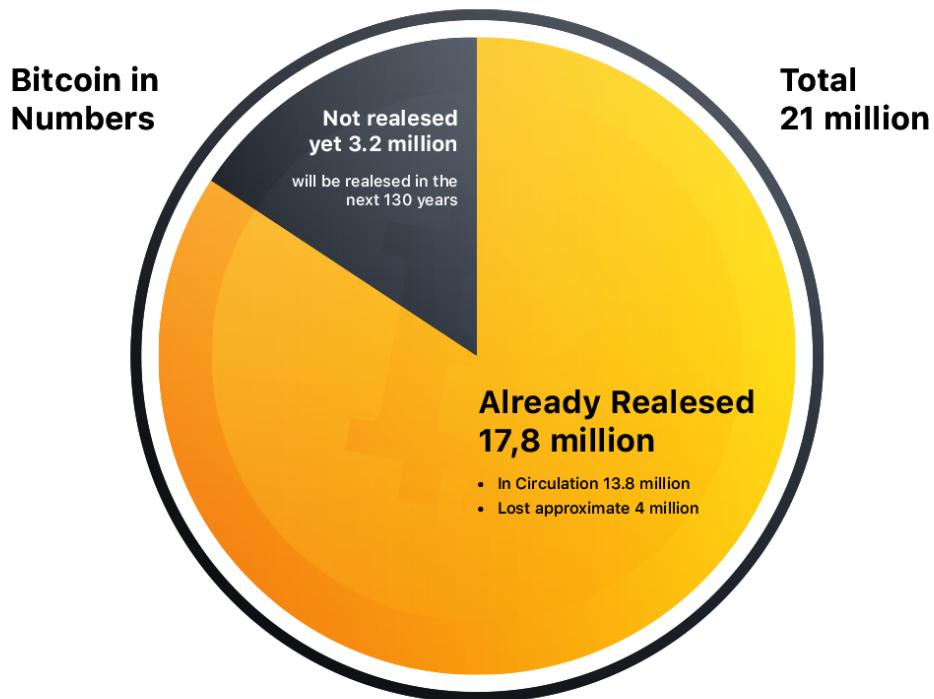


Fig. 4. Proportion of Bitcoin in existence.

But how are new Bitcoins created? In simple terms, the Bitcoin network is designed so that a certain number of Bitcoins are added to the network every 10 minutes. Those newly created Bitcoins are given to one of the nodes on the Bitcoin network. The award goes to the node that is the first to solve a mathematical problem successfully. Although all nodes are trying to solve it, only the first one gets the pay-out. The process of solving the mathematical problem is called mining.

No single entity controls the release of new Bitcoins into circulation. It's an automated process that's regulated by algorithms. The algorithms were coded into Bitcoin at the start of its existence.

Once the total Bitcoin count reaches 21 million, no new Bitcoins will be awarded to the winning node.

Experts estimate that about four million Bitcoins have been already "lost." Typically, coins are lost because users have misplaced their private keys or hard drives containing Bitcoin have been discarded. It is estimated, therefore, that out of 18 million Bitcoins created so far, only about 14 million are available to use.

Further Reading:

- [How Many Bitcoins Are There?](#)
- [Nearly 4 Million Bitcoins Lost Forever, New Study Says](#)
- [The 21 Million Bitcoin Story Explained: Why Is the Number Special?](#)
- [How Many Bitcoins Are Lost vs. How Many Are Hodled](#)

Bitcoin Forks and Other Important Cryptocurrencies

While learning about Bitcoin, crypto newcomers quickly discover a large number of alternative cryptocurrencies already in existence. Many of them portray themselves as a better alternative to Bitcoin.

Moreover, some of these cryptocurrencies have the word "Bitcoin" in their names. It only adds to the confusion.

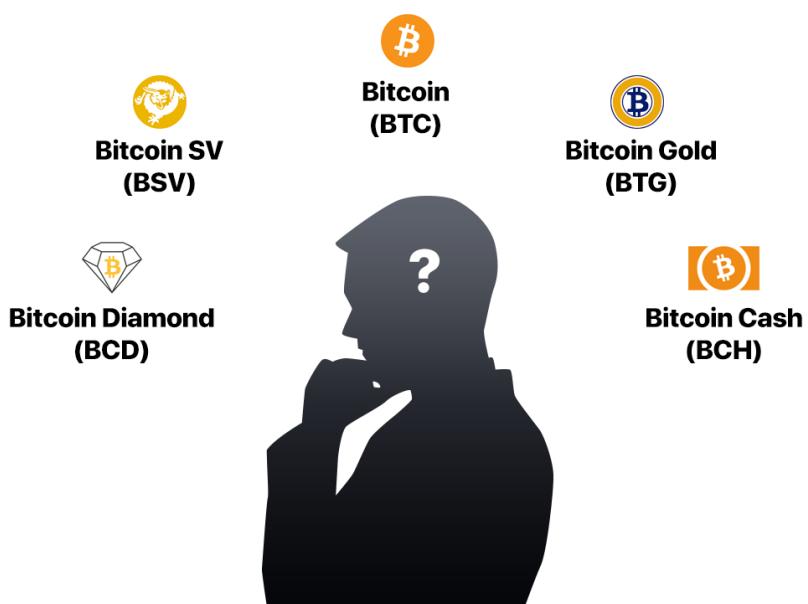


Fig. 5. Examples of Bitcoin forks.

You can subdivide the various tokens in the following three ways:

- **Bitcoin:** The original Bitcoin---created by Nakamoto---has the ticker symbol BTC. It's generally referred to as Bitcoin. You might also see it called Bitcoin Core.
- **Bitcoin Forks:** In addition to Bitcoin itself, there are several other cryptocurrencies with Bitcoin in the name. They are called Bitcoin forks and are cryptocurrencies which were derived from the original Bitcoin (BTC). Due to the open-source nature of Bitcoin, anyone with programming experience can create a Bitcoin-esque cryptocurrency with some modifications, then market it as a separate cryptocurrency. The most noteworthy example is Bitcoin Cash.
- **Altcoins:** Altcoins refers to all other cryptocurrencies that exist. Although there are thousands in circulation, only a few have managed to attract an audience and gain significant market share. The altcoins which have not attracted any audience are generally regarded as coins with no value proposition and are labeled as "shitcoins."

For a comprehensive list of all the cryptocurrencies in existence, check out [CoinMarketCap](#).

Cryptocurrencies ▾		Exchanges ▾		Watchlist		USD ▾	Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	...
1	฿ Bitcoin	\$182,021,025,358	\$10,175.27	\$16,626,430,586	17,888,575 BTC	-4.74%		...
2	♦ Ethereum	\$20,181,377,367	\$187.89	\$7,102,681,308	107,411,051 ETH	-4.78%		...
3	× XRP	\$11,357,014,383	\$0.264790	\$1,095,503,978	42,890,708,341 XRP *	-3.71%		...
4	฿ Bitcoin Cash	\$5,380,432,684	\$299.59	\$1,269,783,876	17,959,300 BCH	-6.01%		...
5	฿ Litecoin	\$4,551,299,586	\$72.15	\$2,651,275,611	63,080,574 LTC	-4.57%		...
6	฿ Binance Coin	\$4,242,951,364	\$27.28	\$224,575,110	155,536,713 BNB *	-3.10%		...
7	฿ Tether	\$4,031,844,692	\$0.997017	\$18,481,641,025	4,043,907,382 USDT *	-0.49%		...
8	฿ EOS	\$3,319,050,367	\$3.58	\$1,397,564,544	928,364,887 EOS *	-1.88%		...
9	฿ Bitcoin SV	\$2,372,870,606	\$132.90	\$292,072,990	17,854,986 BSV	-6.25%		...
10	฿ Monero	\$1,396,773,643	\$81.37	\$68,508,513	17,166,204 XMR	-6.76%		...

Why Bitcoin

Why did Bitcoin grow in popularity? And when (if ever) can we expect to see the growth plateau?

From Idea to Reality

Bitcoin was initially worthless; only a handful of people knew about it. In its early days, the general public mostly perceived Bitcoin as "fun money for geeks" rather than as a phenomenon that could challenge the present-day financial system. Only a few understood the true purpose of Bitcoin. And although a lot more people understand the purpose today, the number is still low in global terms.

The mainstream media played an influential role in shaping how the masses perceived Bitcoin in those first few years. Initially, nearly all media mentions of Bitcoin were negative. Indeed, the technology has been declared dead by various publications more than 400 times!

Back in those first few years, the idea that Bitcoin would someday be worth thousands of dollars appeared outlandish. One early adopter famously spent 10,000 BTC (around \$100,000,000 USD at current prices) on a single pizza.

Fast-forward to October 2019, and Bitcoin is consistently trading around the \$10,000 mark. It's impressive, but in practice, the biggest challenge for Bitcoin was to grow from \$0 to \$100. That didn't happen until 2013, more than four years after its launch. As more time passed, the price went higher and higher. It broke \$1,000 in 2014 and reached an all-time high of \$20,000 just three years later, at the end of 2017.

Bitcoin's price remains exceptionally volatile. Within nine months of its all-time high, the price had dropped back to \$3,000. The volatility is primarily due to the small number of people who are willing to buy and sell Bitcoin at any given time. Even though Bitcoin has a 200 billion market cap, it's still common to see a daily price swing of five percent or more. The market cap of Bitcoin would need to hit the trillions before hype, panic, and large transactions would no longer affect the price.

Further Reading:

- [Bitcoin History](#)
- [A Dazzling History of Bitcoin Ups and Downs](#)
- [What Causes Volatility in Bitcoin?](#)
- [Why Bitcoin Has a Volatile Value](#)
- [The Bitcoin Volatility Index](#)

Today, the perception of Bitcoin is very different from what it was 10 years ago. These days, nearly all mainstream financial channels regularly talk about Bitcoin. And it's not just the media, Wall Street and world leaders are all starting to take notice.

- [Fed Chair Jerome Powell on Bitcoin as a Store of Value](#)
- [President Trump on Bitcoin](#)
- [Jack Dorsey, CEO of Twitter](#)
- [Ron Paul Pledges Allegiance to Bitcoin, Calls Crypto a Great Idea](#)
- [Brian Armstrong, CEO of Coinbase](#)
- [14 Bitcoin Quotes by Famous People](#)

It's no longer perceived as "fun money for geeks" but as a valuable financial asset. The current Bitcoin price, as well as the current market capitalization, is an indication of the new reality.

Why Is Bitcoin Growing?

To understand what drives Bitcoin's growth, it's essential to look at Bitcoin as a social cause. The technology seeks to provide a solution to some major socio-economic and geopolitical problems, rather than merely being a new asset class. Bitcoin is not only an improvement on how we perform financial transactions and preserve wealth. It's a whole new way to own and exercise control over your assets.

Unlike traditional assets and financial instruments, which are generally enforced by governments or other centralized organizations, the core driving force of Bitcoin is its global community. The community is guided by liberal ideals.

Some of the main principles at the core of those ideals are:

- A financial system must be decentralized and tamper-proof.
- A financial network must be unconditionally open for all.
- All participants must have unconditional control over their assets.
- The underlying asset should have scarcity.

In the face of modern-day problems such as excessive money printing, politically motivated sanctioning, for-profit wars, and a centralized financial system, a growing number of people are moving towards Bitcoin.

- [Coinbase Custody Seeing \\$200-400 million in Crypto Deposits Weekly](#)
- [Billionaires Are 'Scouring the Market' to Own 25% of Bitcoin in Circulation](#)
- [Bitcoin Stats: Rich List and Distribution](#)
- [Russia Plans to Tackle US Sanctions With Bitcoin Investment, Says Kremlin Economist](#)
- [Venezuela Smashes Weekly Bitcoin Trading Record With 114B Bolivars](#)

The growing trend in Bitcoin's popularity is likely to continue. Those that understand the changing reality are the ones who are trying to grow their Bitcoin holdings as quickly as possible.

Can the Growth of Bitcoin Be Stopped?

A lot of new people entering the Bitcoin ecosystem remain skeptical about its ability to succeed. The narrative that one day Bitcoin (or a similar decentralized system) may replace centrally regulated financial institutions seems fanciful---especially when the core beneficiaries of the current status quo are some of the most world's most powerful entities.

Many people also assume that governments are going to try and ban Bitcoin. However, those beliefs are founded on a misunderstanding about how Bitcoin operates on a technical level.

So, the real question becomes, "do governments (or other organizations) have the ability to stop Bitcoin?" The answer is no.

Even if a government tries to outlaw Bitcoin, enforcing such a ban would be near-impossible. As long as there is electricity powering computers, phones, and other smart devices, the Bitcoin network can exist and flourish. Yes, lawmakers can make it more difficult for people to participate in the network, but that is the extent of their power.

Taking down the Bitcoin network would be more difficult than taking down the entire internet. While modern-day regulators are able to censor what is being seen on search engines, YouTube, or in mainstream media, censoring people from being able to participate in the Bitcoin network is a new level of complexity.

- [Rep. Patrick McHenry: 'There's No Capacity to Kill Bitcoin'](#)
- [US Lawmakers Are Realizing They Can't Ban Bitcoin](#)
- [Unstoppable Code: The Difference Between Can't and Won't](#)
- [Blockstream Satellite: Broadcasting Bitcoin From Space](#)

The only way for the Bitcoin network to cease having any meaningful value is for everyone to stop using it. Such an outcome would only realistically occur if someone discovered an irreparable fundamental flaw in the code powering the network.

Getting Started With Bitcoin

If you made until this point, you should already have a general idea of what the Bitcoin phenomenon is all about. The next step is to learn how to buy Bitcoin; then you can have some of your own.



At current prices, buying even one Bitcoin would set you back as much as \$10,000. The good news, you don't have to purchase whole coins. So, why not start small and buy only \$50 or \$100 worth of Bitcoin at first? Later, once you're comfortable with all aspects of owning Bitcoin, you can buy more and increase your holdings.

Disclaimer:

Regardless of what anyone says about Bitcoin and its future potential, you should understand that there are no guarantees that the price of Bitcoin will continue to grow. A lot of people believe in the technology and hope it will cement its place on the world stage, but no one knows for sure.

Therefore, use your own judgment when investing in Bitcoin. Keep in mind that it may go down in price and never recover. You should never invest more than you can afford to lose.

How to Buy Bitcoin With a Credit Card

There are two main ways for a newcomer to acquire Bitcoin. You can either find someone willing to send you some or you can purchase some online.

The easiest option is to buy online with a credit card. However, while the option is convenient, you will be purchasing the crypto at slightly more than the market rates (typically around one percent).

Note: There are lots of fake and fraudulent sites that claim to sell Bitcoin. For your safety, only use the resources we've recommended or ones that you have thoroughly researched yourself.

Below, you will find a list of popular places that you can use to purchase Bitcoin and other cryptocurrencies using credit cards. For EU or US residents, any of the options should work without problems. For people living in less developed nations, there will be fewer options to choose from.

- <https://cex.io/cards/>
- <https://payments.changelly.com/>
- <https://www.coinbase.com/>
- <https://www.coinmama.com/bitcoin>
- <https://www.binance.com/en/creditcard>
- <https://buy.bitcoin.com>
- <https://indacoin.com>
- <https://www.bitpanda.com/>

How to Buy Bitcoin on an Exchange

If you want to acquire Bitcoin regularly, you should buy through a cryptocurrency exchange at market prices.

Cryptocurrency exchanges are websites where you can buy and sell cryptocurrencies using fiat money or other crypto tokens. If you're looking to invest a substantial amount of money, buying on a cryptocurrency exchange is the safest option. It may sound complicated for someone who has never traded stocks or currencies, but it's not difficult if you spend some time learning.

When it comes to trading terms and requirements, most exchanges abide by financial regulations and have specific rules and limits in place. Therefore, the steps for purchasing the Bitcoins on an exchange is as follows:

1. Set up an account.
2. Verify your identity using an official ID document.
3. Send funds to your exchange account.
4. Purchase Bitcoin on the exchange.
5. Transfer your purchased Bitcoin to your wallet for safekeeping.

Note: While basic ID documents will work for accounts with a low monthly turnover, once you go higher, you should expect to go through a more robust inspection known as KYC and AML checks. In addition to identity checks, you will be asked to provide documents proving the origin of your funds. Should you fail to do so, your funds and/or account may get frozen.

Listed below are some of the better-known cryptocurrency exchanges:

- [Coinbase.com](#)
- [CEX.io](#)
- [Binance.com](#)
- [ShapeShift.com](#)
- [CoinMama.com](#)
- [Changelly.com](#)

Storing Bitcoin Safely

Bitcoin is stored in cryptocurrency wallets. Wallets come in many different forms. A wallet can be in the form of a mobile app, a desktop program, a website, or even a small hardware gadget.

Bitcoin Wallets Explained

Regardless of the type of wallet and what the wallet's developer is claiming on its website, there is one crucial feature you need to look out for: Whether the wallet lets you (the owner of funds) exclusively control the cryptocurrency held on that wallet. It is the chief security criteria you should look out for when choosing a wallet for your Bitcoins.

To help, you need to know that cryptocurrency wallets can be categorized in three ways:

1. **Non-Custodial:** They give a user exclusive and unlimited control over their crypto funds. The company providing the wallet does not have any control over the assets the user holds. Generally, these types of wallets also enable users to switch between wallets made by different parties without issues easily. These are the preferred type of wallets.
2. **Custodial:** They don't give user exclusive control over the funds. The wallet provider may potentially block a user from spending the wallet funds. Moreover, it's not uncommon for such wallet providers to get hacked and for users to have their funds stolen. Unfortunately, most of the wallets on the market fall into this category. Avoid such wallets whenever possible.
3. **Hybrid:** In a hybrid wallet, neither a wallet user nor the wallet provider has full control over the funds. These wallets are programmed to require approval from both parties for both the owner and the wallet provider. This works well against hacking attempts but keeps the door open for the wallet provider to censor the user.

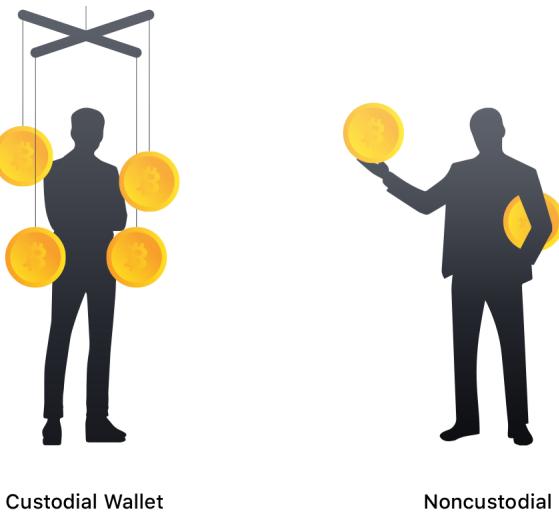


Fig. 6. Custodial vs non-custodial wallets

Non-custodial wallets are considered safer than custodial or hybrid wallet types. It is the only type that provides users with exclusive control over cryptocurrencies held on the wallet.

A lot of people keep their Bitcoin on a crypto exchange. For the most part, crypto exchanges provide users with custodial wallets. Many mistakenly assume that keeping their assets on exchanges is safe. In practice, the complete opposite is true. Just like wallet providers, exchanges are often targeted by hackers. And when exchanges are hacked, users are typically not compensated for their loses.

- [The Largest Cryptocurrency Hacks So Far This Year](#)
- [Coincheck: The Biggest Crypto Exchange Hack of All Time](#)
- [A Timeline of Major Crypto-exchange Hacks](#)
- [Hack Flashback: The Mt.Gox Hack](#)
- [Crypto Developer Komodo 'Hacks' Wallet Users to Foil \\$13 Million Theft](#)
- [9 Ways to Hack Your Bitcoin Wallet](#)
- [Cryptocurrency Customers Are Unable to Access Their Coins After Canadian CEO's death](#)

If you keep Bitcoin on an exchange, it means the exchange keeps your assets in their account. The exchange merely gives you a username and password so you can send instructions to withdraw/deposit your assets. The exchange may freeze funds or restrict access to your account for a multitude of reasons. You're inadvertently placing an enormous amount of trust in the organization.

Understanding the Private Key

The notion of a private key is relevant to non-custodial wallets. Such wallets do not provide users with usual account/password authentication methods. Instead of traditional accounts, non-custodial wallets randomly generate a secure cryptographic key. It is called the private key. Private keys are how you access and exercise control over your funds.

Any entity which has access to the private key has full access to funds in the wallet; it can be considered the wallet's owner.

- Custodial wallets do not provide the user with the private key. The wallet operator has full control over the assets.
- Non-custodial wallets provide the private key to users. The user has full control of the wallet's assets.

The private key is usually shown to users as a series of 12 or more words. The 12 words are a "human-readable" representation of the private key. The actual key is a 256-bit number.

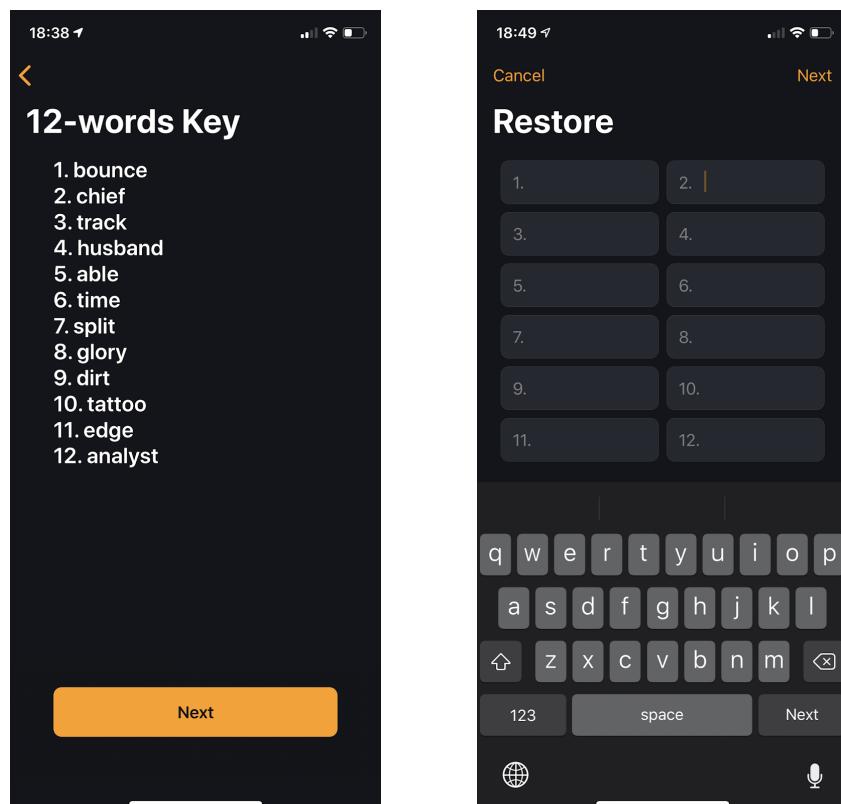


Fig. 7. Sample private key from Unstoppable Wallet

The image above shows a sample private key from [Unstoppable Bitcoin Wallet](#). The wallet associated with the key does not have any funds in it. If it did have funds, anyone reading this guide could import the key on a wallet app, access the wallet, and transfer the funds elsewhere.

Nearly all non-custodial wallets provide an **Import** (or **Restore**) wallet feature. It enables anyone to enter an existing private key and restore access to the wallet's funds. Some wallet apps even allow you to import/restore keys that were generated in other wallets.

The feature means that even if your phone breaks or the wallet app stops working, your funds are still safe; you will always be able to restore access to your Bitcoins using the private key the wallet generated. There are no timeframes---the same key would work years later.

It is clear, therefore, that safely storing your private key is extremely important. Failure to do so could result in a loss of your assets. If you lose the key or unknowingly expose it to someone, they can get control of your Bitcoin. That's the only thing you need to understand. The rest is secondary.

Storing Private Keys Securely

Depending on the tech you use in your day-to-day life, there are a few different ways you could store your private keys.

- **Option 1:** Write your private keys on a piece of paper and store it somewhere offline.
- **Option 2:** (macOS users): You can [store private keys in Keychain's Secure Notes](#).
- **Option 3:** (Windows users): You can [encrypt and protect your private keys using VeraCrypt](#).

Recommended Non-Custodial Wallets

Below are some of our favorite non-custodial wallets. The screenshots shown in this guide were taken on the Unstoppable wallet app.

Wallet Apps:

- Unstoppable Wallet (<https://unstoppable.money>)
- BRD Wallet (<https://brd.com>)

Hardware Wallets:

- Ledger (<https://www.ledger.com>)
- Trezor (<https://trezor.io/>)

Privacy-Focused Wallets:

- Samourai (<https://samouraiwallet.com>)
- Wasabi (<https://wasabiwallet.io/>)

What Happens If You Lose Your Phone?

If you are using a non-custodial wallet app on your phone and you lose your device, what happens? Could someone steal your crypto if they find it?

Both Android and iOS provide security mechanisms to keep sensitive data safe in the case of loss. A quality wallet app will store your private keys by following the storage guidelines recommended by Google or Apple. Typically, that means relying on the PIN code feature.

Of course, there have been many high-profile incidents whereby authorities have tried to unlock a phone's PIN code. They have rarely been successful:

- [FBI–Apple Encryption Dispute](#)
- [Tim Cook: Americans Shouldn't Have to Choose Between Privacy and Security](#)
- [A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?](#)

If the phone doesn't have a PIN lock in place, the person who finds your phone may potentially access the apps on the phone, including the wallet app itself. If successful, the thief could then steal your Bitcoin by sending it to another wallet.

In contrast, if the phone has a PIN, it becomes extremely difficult to hack into. Private keys become unreachable. Reputable wallet apps will not work if the phone's operating system doesn't have a PIN lock enabled.

In the case of device loss, a person can get a new phone and restore the wallet funds by using the 12-word private key. After access to the wallet is restored, it is recommended to transfer the funds to a new wallet.

Using Bitcoin

Now that you understand the importance of the private keys, let's quickly go through the process of sending and receiving Bitcoin. Nearly every cryptocurrency wallet comes with the functionality.

How to Receive Bitcoin

To receive Bitcoin from someone, you need your Bitcoin address. The address is usually located in the **Receive** section of the wallet app. The screenshot below shows the Receive screen on the Unstoppable wallet app.

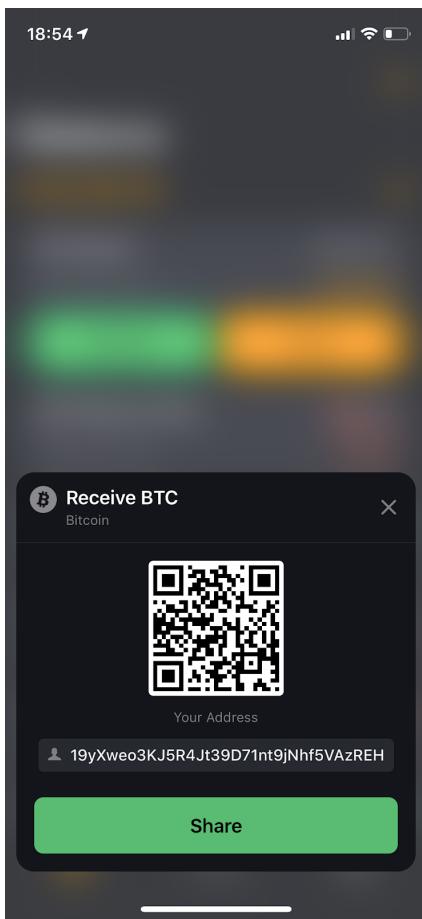


Fig.8. Receiving Bitcoin in Unstoppable Wallet.

You need to copy the address and give it to the entity that wants to send you Bitcoin. It should be noted that most non-custodial wallets will provide you a new address for each transaction. It is a recommended privacy feature. The purpose is to keep your transaction history somewhat anonymous. We'll take a closer look shortly.

Although the wallet will generate a new address after each incoming Bitcoin transaction, older addresses will remain functional and will appear in your wallet whenever someone sends funds to you. In practice, this means that you can generate an unlimited amount of addresses for people to send Bitcoins to you, and all of them will reach you.

How to Send Bitcoin

To send someone Bitcoin, you need to ask the recipient for their Bitcoin address. You then use the **Send** feature in your wallet app to direct the desired amount to the provided address.

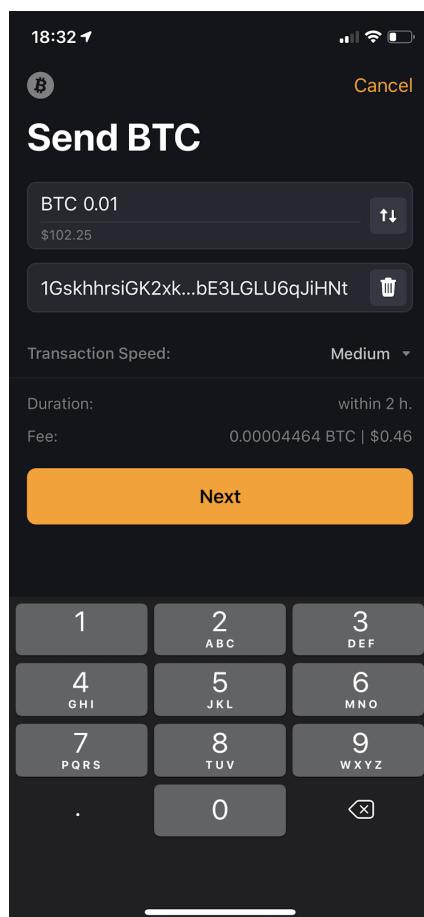


Fig.9. Sending Bitcoin in Unstoppable Wallet.

When sending a transaction, the sender must also pay a small transaction fee. It is awarded to the node which adds the transaction to the blockchain.

Once the user clicks on the Send button, there is a brief period while the transaction remains in a queue. Some wallet apps allow the user to change the transaction while it is in the pending queue.

Note: Bitcoin transactions are final. Once the Bitcoins are sent to the destination address and included in the block, they are non-reversible. Only the owner of the destination Bitcoin address can send or spend the Bitcoin.

How Fast Are Bitcoin Transactions?

What happens to a transaction after the user clicks on the Send button in the wallet? Well, every Bitcoin transaction goes through the following three stages:

1. Pending Phase

The pending phase occurs while the transaction is in progress.

1. A user clicks on the Send button in the wallet app.
2. The transaction reaches the nodes on the Bitcoin network.
3. Each node places the transaction in a queue, called a "mempool."

This phase should be almost instant in most wallets. At the end of the phase, network nodes have the transaction in the queue but not it in the blockchain (the global history of transactions) yet.

When the transaction is sent, the recipient will see it as pending in their local transactions list within a couple of seconds. While it remains pending, it's still technically possible for the sender to modify/cancel the transaction.

2. Confirmation Phase

The next phase happens when the transaction is added to the blockchain and is confirmed by nodes. That usually happens within 10 minutes but can take longer. There are two factors which can affect the amount of time for the transaction to be confirmed:

1. The transaction fee set by the sender.
2. The current number of pending transactions in the network.

When the number of transactions in the network exceeds the amount of transactions nodes can process, nodes get to choose which transactions to include first. In general, nodes give priority to transactions which pay the higher fee. Most wallet apps will take the current network conditions into account and recommend the optimal fee on the Send screen.

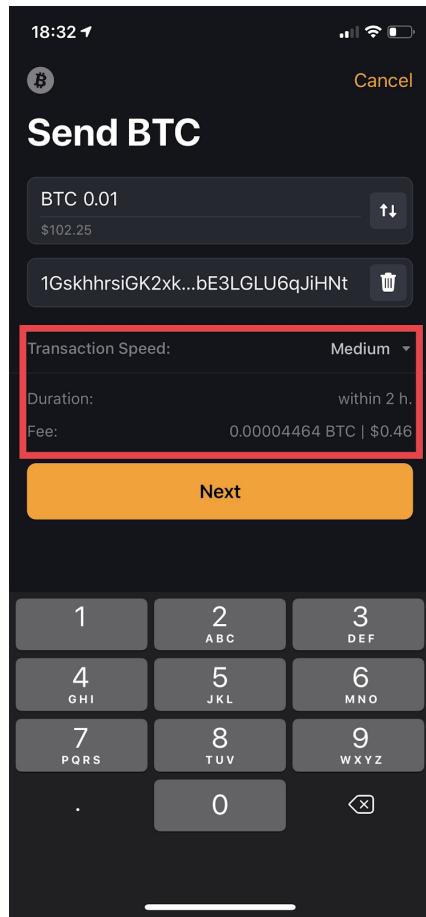


Fig.10. Illustration of transaction speed, duration, and fee in Unstoppable Wallet.

Final Phase

After the transaction is included in the block, it's safe to assume that it is complete. However, due to the nature of how the Bitcoin network operates, it's recommended to wait for between three to six blocks to pass before the transaction can be regarded as final and irreversible.

As soon as the transaction is included in the block, it's considered to have had one confirmation. When the blockchain adds another block on top of it, it's said to have received two confirmations, and so on.

Anyone can monitor the status of any transaction from the moment it was sent using a public block explorer site. In practice, this means that as soon as a user presses the Send button, the receiving party can monitor the transaction online and see how it's progressing. To do so, the receiver only needs the ID number of the transaction. You can obtain it from the wallet.

Below, you will find some of the popular public transaction explorers for Bitcoin network:

- [Blockchain.com/explorer](https://blockchain.com/explorer)
- [BTC.com](https://btc.com)
- [BlockChair.com](https://blockchair.com)

Bitcoin Privacy Explained

Bitcoin is semi-private. Although all transactions in the Bitcoin network are public, they simply appear as a transaction from one Bitcoin address to another.

The image below shows a screenshot of a transaction from the BTC.com block explorer:

The screenshot shows a transaction ID: 75e728201f3c35346542f5671ebefa958191aa64b0567aad46d2a7360b626280. The transaction summary includes the following details:

Summary	Transaction ID
Height	595277
Confirmations	1
Timestamp	2019-09-17 16:38:20
Size (rawtx)	223 Bytes
Virtual Size	223 Bytes
Weight	892
Input (1) 0.20053102 BTC	
Sender: 13dnLo9ySjaTnz7frVbXanAKed7F9BZxhg (0.20053102)	
Output (2) 0.19829102 BTC	
Receiver: 1JYEPEPjmrFQA8LkHc14K4omZxPJmoQfdm (0.09829102)	
38KgKMpoB2r3FvdoV9aioweSiKy4cDX82h (0.10000000)	

Other details shown include Sigops (4), Fees (0.00224000 BTC), Fees Rate (BTC / kB) (0.01004484 BTC), and a link to Other Explorers. A BlockChair logo is also present.

As you can see from the image, there is no way to know the identity of the sender or recipient by looking at an individual transaction. The sender and recipient could even be the same person.

That said, by clicking on the sender's address, it's possible to see which address the sender received the funds from. If the wallet user always uses the same address for incoming transactions, it would be easy to see all incoming transactions and build a comprehensive transaction history.

Conversely, if the wallet user uses a new address for each new transaction, then identifying the user's incoming transactions becomes close to impossible.

Remember, this is an entry-level guide. It is not a complete picture of Bitcoin's privacy features. For an advanced user with a large amount of Bitcoin, or for someone living in a hostile environment, several other factors should be considered.

Further reading:

- A Non-Technical Guide to Privacy in Bitcoin

Using Bitcoin for Purchases

The ability to pay with Bitcoin in stores remains uncommon. While some merchants like Whole Foods are slowly starting to accept payments in Bitcoin, the vast majority of retailers are still not on board. There are many reasons for the lack of adoption, ranging from the absence of legal guidelines for merchants to the technical architecture of the Bitcoin blockchain.

However, there are already some reliable ways to spend your cryptocurrency. For example, some companies provide branded debit cards which can be used to pay anywhere that either Visa or MasterCard is accepted. You pay with a card as you would normally do, and the amount is deducted from your crypto wallet balance using current market rates.



Below, you will see some of the more popular providers of such cards. Most are only available to people living in the US or Europe. They all require the user to provide some identification documents.

- [Crypterium.com](#)
- [Crypto.com](#)
- [Coinbase.com](#)
- [Nexo.io](#)
- [2gether.global](#)
- [Cash.app](#)
- [Cryptopay.me](#)

When using the services, the card provider will issue you with a crypto wallet. It will be a custodial wallet and, therefore, you should never keep too many funds in it.

To reiterate---use a non-custodial wallet for your primary funds and occasionally top up the wallet provided by card provider with small amounts. Think of it as a prepaid debit card.

Bitcoin Nodes and Mining

As mentioned earlier in the guide, over 10,000 nodes are powering the Bitcoin network. The nodes are spread geographically and cover most regions worldwide.

Anyone can set up a node without much effort. The node doesn't require any maintenance and can even operate on an old computer. There just needs to be a working internet connection.

Do You Need to Run a Node?

Nodes are tasked with a) validating every new transaction, and b) broadcasting transactions it receives to other nodes in the network. If one of the nodes tries to cheat the network by marking an invalid transaction as valid, the other nodes will disregard it.

Cumulatively, the nodes guarantee decentralization, availability, and security of the network.

- **Decentralization:** They allow participants to communicate with the network using any node (even their own).
- **Availability:** As long as at least one node is online, the Bitcoin network will remain operational.
- **Security:** The more nodes there are on the network, the harder it is for an entity to cheat. The other nodes would all work against it.

By running a Bitcoin node, therefore, you're contributing to the Bitcoin network and helping to maintain its existence.

Also, keep in mind that there are some countries where Bitcoin currently is considered illegal. Make sure you're aware of the potential risks in your location before you begin.

Different Types of Nodes

While all nodes on Bitcoin Network are equal, some nodes may do more things than others. There are two main types:

- **Full Nodes:** Full nodes keep a complete copy of the blockchain. Any full node can independently verify any transaction for validity.
- **Miners:** All miner nodes continuously compete with each other to be the node that gets to add the next block to the blockchain. The miner node that is the first to solve a mathematical problem is the one that wins the associated Bitcoin reward.

A node can be both a miner and a full node.

The Bitcoin network was designed so that a certain number of Bitcoins are released roughly every 10 minutes. The release happens when a new block of transactions is added to the blockchain. The node that adds the new block to the blockchain gets to keep these newly released Bitcoins. Currently, the reward is 12.5 Bitcoins (reduced by half every four years). The winning node also receives all the individual transaction fees from the new block of transactions.

Is it Profitable to Run A Node?

If you want to run a miner node for the sake of making some money, you need to consider the cost-efficiency of doing so. Making a profit from Bitcoin mining has become extremely difficult for single users due to widespread competition.

Indeed, after taking electricity prices into account, you're very likely to lose money. Mining is generally only profitable for people running a large number of specialized computers and who are buying electricity at industrial rates in countries like China.

Time to Begin Your Bitcoin Journey

That's about it! Now you know all the essential information about owning and using Bitcoin.

Thanks for reading, and please remember to share this guide with people you know who are also keen to learn about the world of Bitcoin.

And remember---this is only an introductory guide. If it has inspired you to learn more about the technical aspects of Bitcoin, we strongly recommend that you read the excellent [Mastering Bitcoin](#) guide by Andreas M. Antonopoulos. He's one of the world's foremost Bitcoin and blockchain experts.

About the author



iBek Esengulov is a co-founder and lead blockchain engineer at [Horizontal Systems](#). He specializes in developing decentralized services built on Bitcoin, Ethereum and EOS blockchains that go beyond the standard cryptocurrency transfer features.

Inspired by emerging notions such as programmable money, decentralized systems, and unstoppable code, he co-founded Horizontal Systems in early 2018. The company is entirely self-funded with a team of 15 senior engineers. Driven by libertarian ideas. Horizontal Systems team builds a new breed of applications which are peer-to-peer and not reliant on any external entity to operate.

Prior to Horizontal Systems, he was the CEO of Grouvi Ltd., a B2B software development company where he led his team in building messenger apps for corporations.

Back in 2007, right out of college, he launched MakeUseOf Ltd. (makeuseof.com) which, in 10 years became the leading consumer tech journal with over 50 professional writers. MakeUseOf serves over 15 million readers every month.

When not working, he spends his time educating people on Bitcoin and public blockchains.