



**BITCOINRODNEY.COM**

**So I'm sending you some free bitcoin education, there is nothing to buy here from me and I'm not an affiliate of anything you may read below.**

**I gathered most of this info from a trusted website and added it here for you so you dont have to scroll the internet to find it. Hope this helps.**

**I'm simply know that there are a lot of you who need to know a lot of this info so you can have the basics of cryptocurrency or bitcoin...**

**Yes, I have some awesome stuff im doing with crypto that is doing well that I have not promoted publicly, so if you do want to be a part of that, please email me back and I can give you a free consultation to see if you're a great candidate for it.**

**So please keep this email handy and save it or make it as important so you can always reference it if needed.**

**Also at the very end of reading this, reply back if this info has helped you.**

Bitcoin is a currency born into the digital age. When using Bitcoin for the first time people should get an idea of how it works. Digital money is different than the traditional finance world is used to. It offers three core values in which many currencies cannot attain: Decentralization, Open Source, and Peer-to-Peer networking. It is important to get an idea of how to use Bitcoin before investing in it or opening a wallet. At Bitcoin.com we are very passionate about the protocol and want to help you learn along the way. There is a lot to learn, but it is not beyond your grasp. Bitcoin is a truly beautiful innovation, and it has the capacity to change the world.

## **Bitcoin: What Is It and why Is It Important?**

### **Who Developed Bitcoin?**

The original Bitcoin code was designed by Satoshi Nakamoto under MIT open source license. In 2008 Nakamoto outlined the idea behind Bitcoin in his white paper, which scientifically described how the cryptocurrency would function. Bitcoin is the first successful digital currency designed with trust in cryptography over central authorities. Satoshi left the Bitcoin code in the hands of developers and the community in 2010. Thus far hundreds of developers have added to the open source code throughout the years.

### **What is the Blockchain?**

Bitcoin is dependent on the blockchain that underlies and structures the system. The blockchain is the vertebrae of the protocol and the glue that holds the network together. It is simply a vast, distributed public ledger of account. It keeps track of every transaction ever made in the network, and all transactions are time stamped and verified by network miners. This is how it works: miners with specialized computers compete to solve mathematical puzzles with other computers, and once they solve a puzzle they are awarded with some Bitcoin, and they also add a “block” of completed transactions to the blockchain for future viewing and verifiability. Once a block is added to the chain the cycle repeats itself, and the computers continue to compete to solve these difficult problems. Every transaction on the blockchain is completely transparent and accounted for in its log. Anyone can see the public keys of any transaction they want (although there are no names associated with transactions). One could go all the way back and view the very first transactions ever made on the first block ever created; this block was called the Genesis Block.

## What is Double Spending?

Double-Spending is the act of using the same bitcoins twice. There is only a 21 million set limit on the protocol and no more can be produced. So the network protects against double spend by the verification of each recorded transaction. The blockchain ledger ensures that the transactions are finalized by its inputs confirmed by miners. The confirmations make each unique Bitcoin and its subsequent transactions legitimate. If one tried to duplicate a transaction the original blocks deterministic functions would change showing the network that it is counterfeit and would not to be accepted.

## How is the Blockchain Different from Banking Ledgers?

### Why Bother with Bitcoin?

That’s the million dollar question, and there’s probably a ton of answers you could give yourself. Are you fascinated by money and technology? Do you want to push the boundaries of money itself and participate in one of the biggest economic experiments of the past century?

At some point you’ll hear people say “Bitcoin is great, but you’ll never use it to buy your coffee every morning”. It’s a sign they haven’t really sat down to think about what money is, or how different people around the world use it. In fact, people are already using Bitcoin to buy their morning coffee and [merchants are using it](#) to accept Bitcoin daily.

Are you [unserved or underserved](#) by the current international banking system because you or your family live in an emerging economy, or freelance for clients overseas? Are you under 18, or work in an industry the credit card companies or PayPal [don’t approve](#) of? Have you ever had an account frozen for some random irregularity, or had to pay over \$20 in international money transfer fees just to send your funds to a friend or loved one? Bitcoin is the perfect solution to all of those issues.

If you’re a merchant – either online or brick-and-mortar – accepting Bitcoin is faster and cheaper than credit cards, and all payments are final. Fees are lower and there’s no risk of fraudulent chargebacks.

Perhaps you think the value of Bitcoin will increase in future and want to invest in it. Or maybe you’ve been reading about the existing fiat currency/central banking and international financial system, realize something’s not quite right with it and want to place control of your money back in your own hands. Bitcoin allows you to do this.

## What is Bitcoin Mining?

Bitcoin mining is analogous to the mining of gold, but its digital form. The process involves specialized computers solving algorithmic equations or hash functions. These problems help miners to confirm blocks of transactions held within the network. Bitcoin mining provides a reward for miners by paying out in Bitcoin in turn the miners confirm transactions on

the blockchain. Miners introduce new Bitcoin into the network and also secure the system with transaction confirmation. They are also rewarded network fees for when they harvest new coin and a time when the last bitcoin is found mining will continue.

## How Can You Buy Bitcoin?

Bitcoins can be bought from various sources. You can purchase them online using an exchange or brokerage service that will enable you to buy Bitcoin with a bank transfer using fiat currency, a credit card, and some services also offer buying opportunities using Paypal. Bitcoin Cash can be purchased locally using [Local Bitcoin](#), and from Bitcoin Teller Machines which are similar to cash ATMs that you find worldwide.

Bitcoin.com has a list of current [online exchanges and brokers](#) who sell bitcoins. You can also buy Bitcoins instantly [using your credit card on Bitcoin.com](#) (the service is provided by [Simplex](#)). Our aim is to provide the best quality services via our website so anyone can easily obtain the cryptocurrency from a wide array of Bitcoin buying/selling platforms.

## Can You Sell Bitcoin?

Bitcoins can be sold in various ways. The currency can be sold online to an exchange or live in person locally. These same instances work similarly to the buying process. You can sell your Bitcoin to the exchange at the current price it's being sold for. More anonymously you can sell in person or use a localized 2-way ATM. ATMs can be found all over the world and these machines are mostly used for purchasing. 2-way ATMs can allow you to sell the currency. Most ATMs however only allow you to buy Bitcoin. There are also teller machines that require identification as well. [Click here](#) to see a list of verified exchanges.

Bitcoin payments are easy to make with a wallet application and addresses. You can use a standard desktop or smartphone to transact with an individual, merchant and exchange. Addresses can be used in number form, in a QR code and contactless technology. Transacting with Bitcoin offers lower fees than any known remittance provider and credit card service. No bank, no state, no third party can offer this low amount of fees.

## Can stores accept Bitcoin?

Brick and mortar outlets can also accept Bitcoin. Services like Coinbase and BitPay offer applications and hardware for the convenience of the store owner. Most of these businesses offer invoicing and accounting with their services. However, third party services are not required by physical merchants to accept the currency. Individual users can also accept Bitcoin directly and handle the transactions and accounting themselves.

## Why Trust Bitcoin?

Bitcoin is a network operating by the three foundational principles of technological freedom: Decentralization, open source code, and true peer-to-peer technology. Bitcoin's trust is based on the subjective valuations of human faith in mathematical algorithms, encryption and numbers. With the three pillars of technological principles Bitcoin's blockchain is a peer-reviewed system of integrity.

## Is Bitcoin anonymous?

Participants in Bitcoin transactions are identified by public addresses – those are the long strings of around 30 characters you see in a person’s Bitcoin address, usually starting with the numerals ‘1’ or ‘3’. For every transaction, the sending and receiving addresses are publicly-viewable.

Since these numbers are virtually incomprehensible, difficult to remember without a computer and don’t contain a person’s name or identifying information, it is often claimed that Bitcoin is an “anonymous currency”. This is also often used as an argument to attack Bitcoin as a currency for example like with illegal transactions.

But it’s not as simple as that. If you publish your address anywhere, it can be linked to your real-life identity. Even if you don’t publish it, simply re-using the same address many times can show a pattern that an analyst with basic skills could link to your identity by looking at transaction times, amounts and regularity – and connecting it to other data sources like receipts, exchanges, and shipped items.

It’s recommended for privacy and security that you use a new address for every single transaction, and most modern wallet software is designed to do just that. But even though this increases the amount of effort and skill required to uncover your identity, it doesn’t make you 100% anonymous. Freely available blockchain explorers and analytical tools have been used to link addresses with only single transactions to other addresses, forming a chain or pattern that eventually reveals its owner. These have been useful in investigating cases of theft at companies like Mt. Gox and Bitcoinica, but can potentially be used to identify anyone.

Due to all of this, it’s more accurate to say Bitcoin is “pseudonymous” and not anonymous. Think of it as a less memorable email address or online handle. Even if it’s not your real name, someone out there can potentially find out who the real person behind the pseudonym is.

There are ways to make Bitcoin more private, but they come with risks. One is to use a “mixer” or “tumbler” which effectively takes your bitcoins and moves them around between a confusing array of addresses until it’s virtually impossible to trace. But do you trust the mixing service to spit your money out the other end, especially since most of them are run by anonymous entities themselves? Usually they do, sometimes they don’t.

Another way is to trade Bitcoin for a digital currency designed to have [greater anonymity](#), like Monero or DASH – effectively making your own mixer. Trade Bitcoin for the other currency, perform one or more transactions to break the link, and trade back into Bitcoin. These transactions increase the complexity, though, and probably require an online exchange, which increases the potential to identify users. Price volatility of all digital currencies may affect how much comes out the other end. And finally – like mixers – if the destination Bitcoin address is one that can be linked to you somehow, the entire process has been pointless.

“Blockchain forensics” is a growing industry with increasing levels of expertise and tool technology. The Bitcoin blockchain is public and permanent record. Your current OPSEC (Operational Security) may beat all methods of investigation available now, but will it stand up to scrutiny in 30 years’ time? How likely is anyone to look? If private transactions are something you care strongly about your operational security should stay as ahead of the curve as possible.

## What Can Bitcoin Do?

The Bitcoin protocol can change the financial landscape we see today. The protocol can act as a currency, voting mechanism, global identification and reputation application, a micro-tipper, crowdfunding platform, initiate trusts, wills and contracts, decentralized domain names, future markets, and basically everything the financial system of today can handle plus so much more. The currency application is just the beginning of this evolution of world’s finances.

## What Happens if I lose my Bitcoins?

Unfortunately, since unique private keys are associated with individual Bitcoin wallets, if the keys are lost, there is ultimately no way to retrieve that key without a passcode seed or other retrieval system; and that key is required to spend those coins. However, most modern wallets have wallet and key backups that you can build prior to storing money. This will allow you to create a new private key so that you may restore your private key on a new wallet if lost.

## Who Is In Charge Of Bitcoin?

Nobody is "in charge" of Bitcoin – at least in the sense that Bitcoin is not a company or organization, has no governing body and no organizational structure. Bitcoin is simply a software protocol, like HTTP (aka the Internet and SMTP (aka email)). This has been the case since Bitcoin's creator, the person (or persons) calling themselves Satoshi Nakamoto, released their creation into the wild in 2009. There are, however, certain groups who can exert influence over the way Bitcoin functions through various means. Again, though, there are no individuals who can claim to speak for these groups and they contain a plethora of opinions and incentives within. Examples of such groups are: **Developers:** These are the people who write and maintain the software the Bitcoin network runs on. Although Satoshi Nakamoto released the first version of Bitcoin himself in 2009, the code has since been re-written and updated by subsequent programmers. The developers choose what updates to make to the protocol, and consider ways it can be improved. **Miners:** These are the people (and companies) that own the machines that generate new bitcoins and keep the network secure by validating transactions. As a result, they [have the power](#) to "vote" with their hardware and choose which Bitcoin software to support. Developers may create and release radical revisions to the Bitcoin protocol, but they'll have no effect unless the Bitcoin miners choose to adopt them. **Users:** That's you. At the end of the day, if regular users decide Bitcoin no longer fulfils their needs, then it will have no value. You can see the user effect in action just by looking at alternative cryptocurrencies collectively known as 'altcoins' – there are currently about 700 different altcoins of varying degrees of popularity. They have risen and fallen in favor as users decided whether to buy, hold, sell, or simply abandon. Merchants have made individual decisions as to whether to accept them as payment or not. Bitcoin faces the same market conditions, and there's no shortage of new projects claiming their protocol is superior. So far none have knocked Bitcoin from its position as the most popular cryptocurrency, but there's no guarantee this will always be the case. Large holders, venture capitalists and influential figures in the "Bitcoin community" could also affect Bitcoin's future path, though their influence is less direct. And again, there is rarely a consensus of vision among them.

## What Is A Bitcoin Wallet?

If you already know and want to see Bitcoin.com's wallet, [click here](#).

Like the name suggests, a Bitcoin wallet is an application that stores, sends and receives bitcoins. You can think of it like you would a leather wallet full of physical cash, and basically that's all you need to use Bitcoin.

The most common wallets are smartphone-based, and use the device's camera to scan QR codes to save the user from needing to copy/paste long Bitcoin addresses. Other people have desktop versions or use browser-based wallets. To the end user the interface is similar, though the way they function and handle private keys (the 'key' which allow you to spend your bitcoins) and user privacy can be very different.

Some apps have features that add value to your Bitcoin-using experience, like location-based Bitcoin business guides, links to exchanges to trade in and out of fiat currencies, more secure vault storage, or the ability to hold digital tokens other than just Bitcoin, such as any number of the many altcoins on offer.

Some wallets have central servers, meaning users have to create accounts with a login name (usually an email address) and password. These are less private and (if login info and keys are not secured properly) may be vulnerable to hackers. On the upside, when a centralized wallet is used if a user forgets their password it's usually recoverable.

Other wallets store all information and private keys on the device itself, some of which generate wallet keys from a single “seed” phrase of about 12 words. If a user remembers the seed phrase, then the wallet can be restored elsewhere if the device is lost or broken. On the downside, if you forget that seed phrase the wallet can’t be recovered.

Apart from smartphone/desktop apps you can also buy [specialized hardware devices](#) to keep your keys completely offline, or even [print a wallet on paper](#) to keep them as safe from hackers as possible. These are the best options for users holding large amounts of Bitcoin.

Bitcoin users now have a wide selection of wallets to choose from and features have improved vastly over the past couple of years. But with more choice comes the need for more caution: fraudulent Bitcoin wallets have begun to appear that mimic the look of popular wallets, but are actually malware that steals bitcoins. Be very careful the wallet you’re installing is the real one.

## Why Does The Bitcoin Price Move So Much?

Until Bitcoin becomes the dominant currency for payments around the world, it will be more popular among traders and price speculators. As a result, the price is subject to the market forces of supply and demand which, at this point in time, goes hand in hand with the trends and whims of speculators – as a result, the price can move suddenly and sharply up or down in response to news events.

As a rule of thumb: if a piece of news makes Bitcoin more likely to be widely adopted, the price rises. If it places extra hurdles towards mass adoption, the price will fall.

You can track all the [latest Bitcoin price movements](#) in real time with Bitcoin.com’s data charts, and convert the price to your local currency with our [instant Price Converter](#).

These events may be based on issues affecting the Bitcoin world only – such as a large scale hack affecting a key Bitcoin exchange, wallet or essential software which causes the price to dip. This happened after the Mt. Gox meltdown in 2014 and thefts at Bitstamp and Bitfinex, plus numerous other smaller companies.

A large market such as the EU, China, Japan or US may announce new regulations either favorable or restrictive to Bitcoin, causing the price to rise or fall respectively (when the Chinese government restricted Bitcoin exchanges’ practices in 2013, the price fell from its record high). It may be an internal issue, such as a miners’ conference or meeting to decide changes to the Bitcoin protocol; the price sometimes dips if a block size or scaling consensus cannot be reached, or seems to be too far off.

News which affects the price may be only vaguely related to Bitcoin, or sometimes not at all. Dramatic economic/financial news like new tax policies, bank runs or bailouts, negative interest rates, stock market crashes, banking instability or government bankruptcies all suggest a new kind of asset class may be preferable, and the Bitcoin price rises.

The price sometimes fluctuates wildly for no apparent reason at all. Sudden crashes, massive increases and up/down volatility can happen and, even after the fact, traders debate over what may have caused it. A large price build-up may suddenly reverse when it hits a certain price level, at which point traders set limit orders *and/or take profits*. *The inverse happens if the price drops too far.*

Some have suggested Bitcoin can never be adopted as a regular currency while prices are so volatile. In truth, if there was a sudden rush to Bitcoin among the general public (maybe due to a crisis in a major fiat currency) the price would probably rise dramatically and then stabilize – especially if there was nothing to swap it for, or no reason to do so.

In the meantime, if you think you can predict the big movements then good luck on the trading exchanges! But be careful, it can also be inexplicable and unpredictable.

## How Can I Trade Bitcoin without an Exchange?

There are plenty of reasons to want to trade Bitcoin for fiat and other digital tokens without an exchange.

The main one is security and trust – two of the largest Bitcoin exchanges of all time, Mt. Gox and Bitfinex, have suffered catastrophic hacks in the past and lost hundreds of thousands of their users' BTC. Not to mention the multiple other smaller exchanges that were hacked or disappeared in mysterious circumstances.

Another is privacy – exchanges these days have similar know-your-customer (KYC) requirements to banks. All this information is kept on file and, like your funds, is at risk of theft if the exchange's security isn't up to scratch.

Person-to-person trading is a small but growing market, with services like [Local Bitcoin](#) facilitating individual trade deals between users. Some also use online classifieds like Craigslist or even chat groups on apps like Telegram and WeChat to indicate willingness to trade in person. Other services like [BitKan](#) have special apps designed to introduce you to online buyers who may not be in your physical location.

Be aware that, in many jurisdictions, even trading with other individuals in a private arrangement is regulated by KYC and anti money laundering (AML) laws, meaning you could be at risk if you don't know anything about the people you're trading with. As such, it is important to clarify your local laws before engaging in person to person trades.

There can also be risks to your personal security from carrying large sums of cash in your pocket or Bitcoin on your device, trading with people you don't know or trust well, trading online, and meeting in private or out-of-the-way locations. Again, it is recommended that you treat your mobile Bitcoin wallet like a regular wallet with cash in it; don't carry more than you would be comfortable losing in case you lose your phone etc.

A third reason to trade off-exchange is volume – if you're looking to [buy or sell large amounts of Bitcoin](#) all at once, a large trade can shift the market against you on low-liquidity exchanges.

## Can I Make Money Mining Bitcoin?

Yes... and no. The days where anyone could make money mining Bitcoin with a desktop computer or GPU cards are unfortunately long gone. The total computing (or "hashing") power of the network has risen exponentially since the introduction of application-specific integrated circuits (ASICs), or machines designed specifically to solve Bitcoin's mining proof-of-work algorithm and nothing else.

For a brief introduction to Bitcoin mining and some basic options, [see Bitcoin.com's guide here](#).

It is still possible for individual miners to make some money by purchasing their own ASIC-based equipment – however, most mining takes place in large factory-like environments with hundreds of machines, in places where energy is cheap (such as China and above the Arctic Circle). And once your machine is superseded by a newer model a few months after purchase, its ability to compete on the network (and thus its earning potential) is greatly diminished, along with its resale value.

You also need to consider energy costs where you live. Bitcoin-mining ASIC machines run very hot and consume large amounts of electricity. You'll need to subtract the costs of electricity and cooling from the profits you make.

However, if you have access to cheap electricity, don't mind (a lot of) extra heat and you think the Bitcoin price is going to increase exponentially in future, try mining for yourself. You'll learn a lot about how the Bitcoin network works, and the network needs more individual miners to keep it secure and decentralized. In fact, a large number of individuals mine Bitcoin to contribute back to the network in this way, as well as just for the fun of it. There's also always the possibility, though increasingly remote, that an individual miner will mine the next block and receive the full 12.5 Bitcoin reward for doing so.

If you still want to mine and don't want to own or manage your own devices, various "cloud mining" companies exist. These are large operations located in data centers around the world. Users buy a share of the mining power available and receive rewards in proportion to their shares. Like all Bitcoin services there are trustworthy and untrustworthy operators, and cloud mining is subject to the same risks and price fluctuations as managing your own equipment – so be sure to [do your research](#) and [ask questions](#) before parting with any money.

## How Can I Sell Bitcoins?

Bitcoins can be sold locally using [Local Bitcoin](#), on Bitcoin brokerages / exchanges, using two-way Bitcoin Teller Machines (BTM's) or you can pay for a good or service with them. Bitcoins can be sold to just about anyone as long as they have a Bitcoin address, and can be sold for any fiat currency in the world or traded for a physical good. Feel free to check out our list of [exchanges and brokerage services](#) to sell your bitcoins online.

## What Can You Buy With Bitcoin?

You can purchase just about anything with bitcoins, from goods like clothing, electronics, food and art to handmade crafts. Bitcoin can also be used to purchase large items like cars, real estate, and investment vehicles such as precious metals. By using [Purse.io](#) users can buy just about anything from Amazon and get a discount of up to 20% just by using Bitcoin. Additionally, many merchants who accept Bitcoin also give discounts for people who pay with the digital currency. Show your friends how easy it is to use bitcoin – head over to our own [bitcoin.com Store](#) and buy a T-shirt, hoodie, bag, all kinds of accessories, even art and bitcoin wallet hardware.

For merchants that don't accept Bitcoin, there's still a way to use your cryptocurrency to purchase the items you're interested in by using a Bitcoin debit card. Bitcoin.com has a list of [Bitcoin debit card companies](#) to choose from; some cards can only be issued to certain countries, and all have varying fees so be sure to read up on your options in order to choose the best card for you.

For cryptocurrency enthusiasts, Bitcoin.com also has its own store which sells Bitcoin-related merchandise such as T-shirts, artwork, coffee mugs, Bitcoin famous Alpaca socks and more. If you're looking for some Bitcoin swag make sure you head over to our [store](#) to find quality items that make great conversation pieces and show off the Bitcoin spirit.

## What Is a Bitcoin Address?

A Bitcoin address is a long string of 27 - 34 numbers and letters that acts similarly to an email address. The address enables the Bitcoin blockchain to recognize when bitcoins are sent and received. These addresses can be used by anybody, from single individuals to businesses to multiple people accessing the one address if desired. It is also considered more secure not to re-use addresses but rather to use a unique address every time you send and receive bitcoins. This increases the privacy of your transactions to a degree and helps in avoiding public tracking of your funds.

## How Do Bitcoin Transactions Work?

Bitcoin transactions are composed of an amount, an input (sending address), an output (receiving address) and private keys (the keys which allow you to spend your bitcoins). A user simply enters a receiving address and if the person possesses the private key associated with the bitcoins they are trying to spend the transaction is sent and verified with the help of miners confirming blocks of exchanges (transactions) within the Bitcoin blockchain. The blockchain is a database of all recorded transactions since Bitcoin's inception.



## What Is A Public Key?

Every Bitcoin address contains both a public and a private key. The public key allows others to send bitcoins to your address, and verifies the signature of the transaction to ensure everything is in order and finalizes the transaction. The private key, on the other hand, allows you to 'unlock' and spend your bitcoins. It does this by signing transactions, which tells the Bitcoin network that you are indeed the owner of the address in which the bitcoins are held and that the transaction is valid. Whoever holds the private key for a Bitcoin address is able to spend the bitcoins which that address holds, so in a very fitting analogy your private key is essentially the key to the safe which is holding your bitcoins. You can also use the private key of an address to sign a message, verifying that you are the owner of the bitcoins held at any given address. This is all secured through mathematics, using asymmetric cryptography.

## How To Accept Bitcoin Payments For Your Store?

It is very easy for any merchant to accept Bitcoin, and most of the time preparing to add the feature to your payment services takes less than 10 minutes. Merchants can accept Bitcoin both online and at physical locations by using a [merchant service](#) payment provider like Bitpay, or even just using a simple wallet address generated on their own device. Bitcoin has significantly lower fees than PayPal, credit card companies and bank services making it far more appealing to store owners than the legacy payment card processors. The cryptocurrency is also irreversible so chargebacks are not possible, and this leaves the decision to refund fully within the hands of the store owner. Merchants can accept Bitcoin through a payment processor, through a Point-Of-Sale (POS) device or simply using their own tablet or smartphone. Adding Bitcoin as a payment method for your store can also increase your customer base for those who like to pay with cryptocurrency as well as broadening your company's reach into the global market. Read more about merchant solutions [here](#).

## What Are The Fees Involved?

There are fees involved with sending Bitcoin called the 'Miner's fee.' Fees are paid to the miners in order for them to verify and secure Bitcoin transactions within the network. A website / developer's solution named '21' offers an online guide detailing the fees within the network for certain time frames. Typically, a larger fee will confirm faster than a relatively low one.

## What Does "Unconfirmed Transaction" Mean?

An unconfirmed transaction is a transaction in the network that the miners have yet to confirm. Typically, confirmations take roughly 10 minutes. However due to the increased popularity of the Bitcoin network confirmation times have increased quite a bit and can sometimes take up to an hour or more. There are solutions in the works to deal with this issue, as well as a lot of discussion within the Bitcoin community around the best way to go about it. If a transaction fails to confirm after 72 hours, the funds will be sent back to the original sender's wallet.

## Is Bitcoin Legal?

Bitcoin is legal in most jurisdictions in the world but there are a small number nation states that have banned its use, such as Ecuador. Wikipedia has a great guide on how Bitcoin is treated in all the countries around the world and explains

regulatory policies surrounding it. Regulations vary from one border to the next so you should always research your location's laws before participating in the network.

## **Who Is Satoshi Nakamoto?**

Satoshi Nakamoto is a pseudonym/name of a person or group of people who created the original Bitcoin client and author of the original reference white paper which details the protocol. Nakamoto participated in the network by helping with the code and mining until 2010 when he/they disappeared, never to be heard from again.

## **How To Make A Bitcoin Paper Wallet?**

Paper wallets are a great way to keep Bitcoin offline and out of hackers' reach. Creating paper wallets is easy but losing the paper also means the bitcoins are lost forever so be careful. Paper wallets contain both private and public keys which allow you to spend your bitcoins. The most common way that people create paper wallets is using [paperwallet.bitcoin.com](http://paperwallet.bitcoin.com) where users can generate a fresh new Bitcoin address and related private key. The website will ask the person to initiate some steps and are then given both public and private keys after the process. After printing a copy, you can load as much bitcoin as you want into your public QR-code. This service, however, does come with a caveat. There are any number of technical reasons why generating a private key on a machine that you don't control is a bad idea; these range from man-in-the-middle (MITM) attacks to untrustworthy site operators, and everything in between. However, downloading the Bitaddress code and running it on your own machine offline can mitigate these risks. This can be further secured by doing so on a machine that is not (and has never been) connected to the internet.

## **How Does The Blockchain Work?**

The blockchain records all of the newly minted bitcoins rewarded to miners who find blocks. Blocks are sets of sent/received transactions that miners confirm for the network. As these actions take place within the Bitcoin protocol the blockchain acts as a ledger of account for all transactions undertaken within the Bitcoin network.

## **What Is A Full Node?**

Full nodes validate transactions within the blockchain and are voluntarily maintained by individuals, groups and organizations (such as merchants for example) all around the world and broadcast all the messages within the protocol. Full nodes add an additional layer of security for these participants within the Bitcoin network and operate in an altruistic manner meaning they work without reward. Some use cases for individuals or groups such as merchants running a full node is for detecting double-spends or for increased privacy.

# **Bitcoin Glossary**

Bitcoin Cash is changing the way people think about money. In order to help you learn about this revolutionary electronic cash system we have compiled a list of frequently used Bitcoin terms below. Note: the majority of these terms apply to both Bitcoin Cash (BCH) and Bitcoin Core (BTC). Read more about the [differences between Bitcoin Cash and Bitcoin Core](#).

**Address:** A string of letters and numbers that people use to send bitcoin to or from. A bitcoin address is shared from one user to another user so that they can send you Bitcoin. Likewise, if you want to send bitcoin to someone you will need their address (obtained from their [wallet](#)).

**Bcash:** A derogatory term created by a resentful minority to try and smear Bitcoin Cash on social media, used to avoid associating BCH with the word 'Bitcoin'.

**BCC:** A ticker symbol for Bitcoin Cash; used mostly on Asian exchanges.

**BCH:** The most used abbreviation and exchange ticker symbol for the Bitcoin Cash digital currency.

**Bitcoin:** An [electronic peer-to-peer cash system](#). There are two main versions of Bitcoin: Bitcoin Cash (BCH) and Bitcoin Core (BTC). BCH is digital money and offers very quick transaction times with low fees. BTC is no longer useful as money because of extremely high fees and slow transaction times.

**Block:** A group of Bitcoin transactions that have taken place during a specific time period. The average is around 10 minutes. Miners process Bitcoin transactions not one-by-one but in groups or "blocks".

**Block Reward:** An amount of Bitcoin that miners earn upon creating a block (of pending transactions). The reward is equal to the sum of 1) the block subsidy (newly 'minted' satoshis) plus all transactions fees attached to transactions included in that block. The subsidy reward is halved every four years.

**Blockchain:** The decentralized, public ledger of each and every Bitcoin transaction that has ever occurred. As blocks are verified by miners, they are added to the chain of previous blocks, hence the name.

**BTC:** An abbreviation and exchange ticker symbol for the Bitcoin Core currency.

**Centralized/Centralization:** A form of organization whereby a single party, group, authority is in control. These systems have single points of failure. VISA, Paypal, ApplePay are examples of centralized payment systems. Centralized organizations are contrasted by decentralized systems.

**Coinbase:** A unique type of Bitcoin transaction with no inputs that is created by miners after finding new blocks. This type of transaction is, in most cases, the first transaction within new a block. Coinbase transactions reward miners for their work.

**Cold Storage:** A way to hold or store a digital asset offline—without connection to the internet. Typical cold storage includes USB drives, offline computers, or paper wallets. Cold storage is the safest method of storing your cryptocurrency especially for wallet balances that you plan to keep untouched for a significant period of time.

**Confirmation(s):** A bitcoin transaction is confirmed once it has been included in a block on the blockchain by a miner. Each subsequent block added to the blockchain is another confirmation for that transaction. 6+ confirmations is generally accepted for a transaction to be finalized although 99.99% of the time Bitcoin Cash transactions can be considered final with 0 or 1 confirmation.

**Cosigner:** A person or entity that has partial control over a multi-signature Bitcoin wallet. To complete a send of bitcoin, a multi-sig wallet requires authorization from a certain amount of all cosigners on the wallet. The amount of authorizing cosigners required is known as 'M of N'.

**Cryptocurrency:** A digital currency that uses cryptography to provide security and verify transactions on its network. Bitcoin is the first cryptocurrency. Unlike traditional fiat currencies, a cryptocurrency does not require a central bank or any other centralized authority to ensure security or to maintain control of money supply.

**Cryptography:** The practice and study of techniques for secure communication in the presence of third parties. Bitcoin and other currencies are related to cryptography insofar as they use mathematics to secure information. Within Bitcoin, cryptography creates and secures wallets, signs all transactions, and verifies each and every transaction on the blockchain.

**Decentralized:** A form of organization which does not require any single party, group, or authority to control services. Bitcoin is a decentralized network because no company, government, or individual created or is in control of it. Bitcoin's governance relies on the community and its code is open-source.

**Distributed:** Also known as peer-to-peer (p2p). A distributed network does not require users to connect to any central server or entity. In a distributed network, users connect directly to each other. Bitcoin is a distributed network that does not have any central processing entity.

**Encryption/Encrypt:** The Bitcoin network uses cryptography to secure wallets so that only those in control of the private key associated with that wallet may access it to send Bitcoin from that address.

**Exchange:** A service, usually a website, that allows users to buy, sell, and trade cryptocurrencies.

**Hash:** A mathematical process miners use on blocks to secure the network and maintain network security. "Hash" also refers to the unique identifier of a Bitcoin transaction.

**Hot Wallet:** Any Bitcoin wallet running on an internet-connected device is considered "hot" (as opposed to an offline or "cold" wallet). Hot wallets should be secured by users since the funds on these wallets are subject to security compromise from hostile users on the network.

**Ledger:** A list of IDs, transactions, time-stamps, balances, and other data related to a financial account. The Bitcoin blockchain is unique ledger in that it is distributed, decentralized, and public.

**M of N:** The requisite number of cosigners needed to provide signatures (M) out of the total amount of cosigners (N) within a multi-signature wallet. A common M of N value is "2 of 3". This means of the three cosigners, any two are needed to authorize a signature.

**Miner:** A specialized Bitcoin user comprised of a computer or group of computers that 1) collect pending transactions into blocks in order to process them and 2) verify blocks created by other miners. Miners are incentivized to perform this work because they collect all transaction fees (attached to transactions within blocks) and are rewarded with new bitcoins as part of the block reward.

**Multi-Signature:** Also known as 'multisig'. These are bitcoin transactions that require authorizing signatures from multiple parties. [Bitcoin.com wallets](#) offer the multisig feature.

**Node:** A special participant on the Bitcoin network. Nodes hold a copy of the blockchain ledger and relay new transactions to other nodes.

**Open Source:** Freely distributed software the code of which is available to the public to edit, use, and share. The Bitcoin code is open source.

**Paper Wallet:** An offline, cold storage, wallet where private key(s) are printed onto a piece of paper or manually attached to some other physical medium for offline storage. This is one of the most secure ways of holding a cryptocurrency.

**Peer to Peer:** A type of network where participants communicate directly with each other rather than through a centralized server. The Bitcoin network is a peer to peer network.

**Private Key:** A string of numbers and letters that is used to spend bitcoins held on a specific Bitcoin address.

**Proof of Work:** Refers to a portion of data which is difficult (i.e., high in resource cost and time-consuming) to produce yet easy for others to verify and which satisfies some requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required *on average* before a valid proof of work is generated.

**Protocol:** A set of official rules which govern how participants on a given network must communicate. Bitcoin's protocol dictates how each node connects with the others, the supply of Bitcoins at a certain time, and also defines other aspects of the network.

**Public Key:** A string of letters and numbers that is mathematically derived from a private key. Public keys allow one to receive bitcoins from other users.

**QR Code:** An image, usually square, that digitally represents a bitcoin public or private key. QR codes are similar to barcodes found on physical products and can be scanned by digital cameras on smartphones or computers.

**Signature:** A portion of a Bitcoin transaction that proves that the owner of the private key has approved the transaction.

**satoshi:** The smallest divisible unit of one bitcoin. There are 100 million satoshis (8 decimal places) in one bitcoin. One satoshi = 0.0000001 bitcoins.

**Satoshi Nakamoto:** Author of the [Bitcoin Whitepaper](#), published in 2008. Nakamoto is considered the founder and creator of Bitcoin. **SHA-256:** The specific hash function used in the process of mining to secure bitcoin transactions.

**Transaction:** An entry in the blockchain that describes a transfer of bitcoins from address to another. Bitcoin transactions may contain several inputs and outputs. Abbreviated as 'tx' e.g. Usually, the first tx within a block is the coinbase.

**Transaction Fee:** Sometimes called the "miner's fee". The transaction fee is an amount of bitcoin included in each transaction by users and collected by miners. These fees are used to incentivize miners to add the transaction to a block. Bitcoin Cash (BCH) fees are considerably lower than Bitcoin Core (BTC) fees.

**XBC:** A ticker symbol for Bitcoin Cash used to meet the International Standard for currency codes (ISO 4217). **Wallet:** A collection of Bitcoin private keys used to spend bitcoins.

Thanks for being a loyal email subscriber. We appreciate hearing from you. Let us know if you ever have any questions.

---

**\*\*Disclaimer\*\*** “You should not buy any crypto currency products unless you are prepared to sustain a total loss of the money you have invested plus any commission or other transaction charges. This material is subject to change without notice. This document is for information and illustrative purposes only. It is not, and should not be regarded as “investment advice” or as a “recommendation” regarding a course of action, including without limitation as those terms are used in any applicable law or regulation. This information is provided with the understanding that with respect to the material provided herein (i) Rodney Burton, Bitcoin Rodney, or The Bit Group, LLC is not acting in a fiduciary or advisory capacity under any contract with you, or any applicable law or regulation, (ii) that you will make your own independent decision with respect to any course of action in connection herewith, as to whether such course of action is appropriate or proper based on your own judgment and your specific circumstances and objectives, (iii) that you are capable of understanding and assessing the merits of a course of action and evaluating investment risks independently.”