

Complete Guide to Bitcoin in 2021

With the growing public interest and increasing rates of Bitcoin, you may have been curious to learn more about this currency as well. I have put together this article using up-to-date and reliable facts to help you understand what Bitcoin is, and how safe it is to use. I hope you find it useful and informative.

Table of Contents

[What is Bitcoin?](#)

[Who is Satoshi Nakamoto?](#)

[Bitcoin transactions](#)

[Blockchain](#)

[Timestamp Server](#)

[Rise & Fall and the Rise of Bitcoin](#)

[How does Bitcoin work?](#)

[How does Bitcoin mining work?](#)

[Bitcoin Mining](#)

[What will happen when all Bitcoin is mined?](#)

[Where to use Bitcoin?](#)

[How to buy Bitcoin?](#)

[How to invest in Bitcoin](#)

[How to Open a Bitcoin Wallet?](#)

[Different and secure options to open a Bitcoin wallet](#)

[Should I buy Bitcoin or not?](#)

What is Bitcoin?



Originally created in 2008 by two programmers going by the names Satoshi Nakamoto and Martti Malmi, Bitcoin is the very first “cryptocurrency” in the world – and also the best known and most valued of over 5,000 known cryptocurrencies today. It was launched to market use in 2009 and since then it has been the top cryptocurrency in the world, in terms of both per coin value and market cap.

Basically, Bitcoin is a decentralized variety of digital currency that you can use to buy, sell, and exchange directly without involving any traditional intermediaries like governments or banks to carry out financial transactions. Bitcoin functions with the help of a

combination of peer-to-peer technology and software-driven cryptography.

Software-driven cryptography is basically a branch of technology which deals with passing secret information that can only be accessed by the sender and the receiver.

Thus, Bitcoin is a unique form of currency that has its foundations in code instead of physical valuables like silver or gold. Even more noticeably, it has nothing to do with central authorities like the American dollar or Japanese yen. In the words of Satoshi Nakamoto, Bitcoin was originally developed because of the need for “**an electronic payment system based on cryptographic proof instead of trust**”.

- Bitcoin is a digital currency that has its own monetary value similar to a commodity. Bitcoin works completely live with internet access and its exchange rates do not depend on any bank.
- Bitcoin is a peer-to-peer currency, a.k.a. blockchain currency, that can be used anywhere in the world using a peer (Internet) connection. Bitcoin works on the basis of peer-to-peer networks, which are not maintained by central organizations or banking institutions.

Who is Satoshi Nakamoto?

Satoshi Nakamoto (**The Creator of Bitcoin**) supposedly began working on the concept of Bitcoin in 2007. No one knows who Satoshi is or if Satoshi is a collective of several people. The Bitcoin

community's general consensus is that 'Satoshi' is a person living in Japan, but that can be disputed as well.

- According to Satoshi's Bitcoin Foundation account, 'Satoshi' is in his late 40s now and lives in Japan – however, there is no way to validate that information.
- The anonymity behind 'Satoshi' exactly expresses what Bitcoin is attempting to create. An anonymous peer-to-peer currency that is tracked by no one, yet transparent enough for the public to see at the same time.
- Many people debate over who Satoshi Nakamoto actually is and disregarding Newsweek's article that they found the real Satoshi Nakamoto living in California in their notorious article in 2014: [The Face Behind Bitcoin](#).
- There are several theories that Satoshi could be a joint effort between **Samsung**, **Toshiba**, **Nakamichi**, and **Motorola** and that these companies together created Bitcoin.
- On August 15, 2008, three people filed a patent for encryption application; Neal Kin, Vladimir Oksman, and Charles Bry. One intrepid researcher, Adam Peneberg, cross-referenced phrases from the patent application and the Bitcoin white paper. The phrase "computationally impractical to reverse" matched both the patent application and the Bitcoin white paper.
- Furthermore, the domain name for Bitcoin's official website, bitcoin.org, was registered three days after the patent application was filed. Additionally, the patent was registered in Finland, where one of the patent authors traveled to 6 months before the domain was registered.

- Unsurprisingly, all three authors adamantly denied the accusations. All possible identities of Satoshi have been vehemently denied.
- It is possible that we may never know the true identity of Satoshi Nakamoto.

Bitcoin transactions

A Bitcoin is, in essence, a chain of digital signatures. To send Bitcoins to another person, the owner of the coin is actually digitally signing a hash or a long string of numbers, that include the details of the previous transaction and the public key. Think of your public key or public address as an email address. The person being paid then verifies the signatures to authenticate the chain of ownership.

Common questions surrounding bitcoin include: “How does a person receive payment?” or “How does a user or a merchant make sure a coin wasn’t **double spent** or used in another transaction before?”

In traditional financial systems, a **trusted third party** is used to hold and verify transactions. **That third party is usually a bank or a money transmitter** who later takes a sizable fee from the transaction. **Bitcoin was meant to be decentralized and to not put trust in a third-party organization.**

Bitcoin was meant to put trust in computers, cryptography, and mathematics. To replace a third-party organization like a bank or a government, Satoshi implemented a transparent, **timestamp server**, which is the backbone of the **blockchain**.

Blockchain

The blockchain is essentially, you guessed it, a chain of blocks. But is much more than that. To put something in the blockchain is a digital equivalent of setting it in stone and digitally recording it forever.

- The longer the blockchain is, the more work a miner will be required to do in order to change a single transaction. This made a very attractive for people that want to store data long term, as it's very unlikely that it will be altered or otherwise changed.
- The blockchain isn't just set to storing transaction records. The blockchain enables a user to store any digital files including artwork, contacts, images, etc.
- The blockchain authenticates that a certain user is indeed the owner of your work and cannot be disputed.

Every Bitcoin transaction ever made in history is noted on a public ledger on Blockchain that anybody can access freely. Thus, it is more or less impossible to reverse or fake a transition. As mentioned above, bitcoin does not depend on a centralized system of banking. Thus, users are not required to identify themselves when carrying out a Bitcoin transaction. When a transaction is initiated, the protocol automatically checks whether the sender has the required Bitcoins and authority to send them.

Bitcoin is considered to be "pseudo-anonymous" – every user is identified by using the address of their wallet, and their transactions can also be traced using this method. However, since cryptocurrency wallets are not limited to online services like exchanges, it can be quite hard to trace a wallet created by an

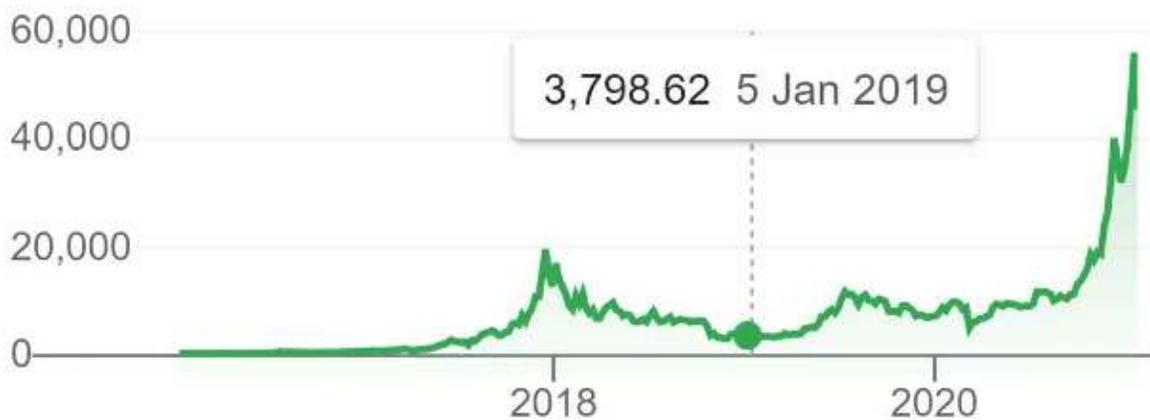
anonymous user on a particular computer. Some pioneers of privacy are also concerned about the complete transparency of every transaction on the network.

Timestamp Server

A timestamp server works by taking the hash of a block of items that need to be timestamped and publishes the hash worldwide. In doing so, timestamps verify that the data needed to make the hash did indeed exist at that time, therefore authenticating the transactions.

Each sequential timestamp includes the hash of the previous one, creating a chain that is strengthened with every timestamp. The question now is, “How do we make this timestamp server decentralized?” In Bitcoin and many other cryptocurrencies, they use a “**proof**”.

Rise & Fall and the Rise of Bitcoin



Bitcoin's Price Graph — 2016-2021

The value of Bitcoin has continued to steadily rise since its creation.

Today's rate of Bitcoin is \$61,734.50 and the total market value of Bitcoin is \$1,153,450,855,132.00.

Its supply is limited to 21 million coins and no more than 21 million coins can be mined. That is why its price keeps rising with time.

Quick Facts about Bitcoin:

- **Today's Rate:** \$61,734.50
- **Total Market Capitalization:** \$1,153,450,855,132.00
- **Total Supply:** 18,684,056

How does Bitcoin work?



The core concept that Bitcoin is based on is a distributed digital record known as a “blockchain”. Basically, a blockchain is a linked body of data that is composed of several smaller units known as blocks. These contain the details of every Bitcoin transaction, such as the total value, buyer and seller, date and time, and a special code to identify every exchange. A digital chain of blocks is formed by putting together entries in chronological order.

After becoming a part of the blockchain, a block can be accessed by any person who wants to view it. Thus, it serves as a public ledger of cryptocurrency transactions. Blockchain is decentralized and more like a Google Doc, which can be accessed and edited by anybody who possesses a link to it. I realize that this concept of anyone editing the blockchain sounds extremely risky. However, paradoxically, that is what makes Bitcoin exceptionally secure.

To make things more clear, here's a more detailed explanation. A transition block cannot be directly added to the Bitcoin blockchain. Instead, it needs to be verified by the majority of all Bitcoin users first. There are also special codes to identify users' wallets and transactions, which must match the correct encryption pattern. These codes are long and random numbers, and thus it is more or less impossible to reproduce them using illegal means.

According to Bryan Lotti of [Crypto Aquarium](#), the chances of a criminal correctly guessing the key to your Bitcoin wallet are about the same as someone winning a Powerball lottery straight for nine times consecutively. Thus, this statistical randomness of blockchain verification codes ensures that the risk of illegal Bitcoin transactions is minimal.

How does Bitcoin mining work?

You're probably familiar with gold miners. Well, bitcoin has miners as well. These miners 'mine' bitcoin. How? Using 'Mining Rigs' to solve complex mathematical algorithms. If you have seen miners and their rigs, with usually several high-end graphics cards on one motherboard, you are seeing proof of work going on. Otherwise known as "mining", which will be discussed more in-depth later on.

Bitcoin Mining

Mining is the process of finding a hash that correctly satisfies the proof of work of a block, verifying the transactions and maintaining the blockchain. While mining can be done theoretically with anything that supports SHA-256, and in the earlier days, it was with CPUs

and GPUs, the most efficient way of doing it now is using **ASICs** or application-specific integrated circuits.

Proof of work is the process of looking for a value that, when hashed with the correct algorithm, in this case SHA-256, that the hash begins with a number of zero bits.

For the timestamp network to work and verify transactions, Bitcoin has included a 'nonce' as well. A nonce is a value that when included in the block, the hash of the block contains a certain number zeros somewhere in the hash.

When the block's proof of work are correctly satisfied, they are then added to the chain. A blockchain is created as more and more blocks are chained together. The longer this blockchain is, more work is required for a malicious entity to reverse a transaction, as it must redo the work of all the blocks.



The Bitcoin protocol asserts that a total of 21 million Bitcoins will exist at a certain point in time, which is the maximum possible number. People who mine Bitcoins simply bring them out into the light, just like gold is dug up from underground in real life. After all these Bitcoins have been mined, there will be no more new coins coming out unless there is a corresponding change in the Bitcoin protocol. Bitcoin miners are paid in the form of transaction fees for producing blocks of verified transactions and adding them to the blockchain.

Also, there is a new concept which is known as **Bitcoin mining pools**. Basically, you can choose to either mine solo or join a mining pool of members. Both these options have their own unique pros and cons. If you work alone, you will not have to share your reward

with anyone, but you have a much lesser chance of solving a block and obtaining a reward. If you join a mining pool, you have a much greater chance of getting a reward, but it will be distributed among all the members of the pool.

What will happen when all Bitcoin is mined?

Experts have claimed that by 2140, all Bitcoins will be mined and may have gotten into circulation. Thus, there will be no more new coins to be gained from Bitcoin mining. As a result, people who depended on mining will have to shift their focus to transaction fees.

Where to use Bitcoin?

In the US, Bitcoin is often used as an alternative form of investment to add variety to a portfolio alongside bonds and stocks. Although it is technically possible to make purchases using Bitcoin, the number of vendors who accept it is pretty small. However, there are certain well-known companies which accept Bitcoin as well. Some of these include AT&T, Twitch, and Overstock. If you look hard enough, you might come across some small websites or local retailers who accept Bitcoin as well.

There are, in fact, quite a few outlets where you can spend your bitcoin. HSB, a well-known insurance company, carried out a survey in 2019 which revealed that over one-third of American small and medium-sized businesses accept cryptocurrency, and nearly 59% of them buy digital currencies for using themselves. In the same year,

AT&T became the first prominent American mobile carrier to accept cryptocurrency payments through BitPay.

You can use Bitcoin to pay for hotels and flights via CheapAir, Surf Air, and Expedia. You can buy presents using Bitcoin as well, such as gift cards via eGifter or Gyft. Bitcoin can also be used in Microsoft's app stores to download app-based services, games, and movies. Similarly, Twitch offers its users to pay for subscriptions using Bitcoin and Bitcoin cash. American customers can purchase fresh pizza from PizzaforCoins using Bitcoins. There are even certain charities and crowdfunding sites which accept Bitcoin, such as Fidelity Charitable, BitGive, and BitHope.

Recently, PayPal announced that they will be enabling cryptocurrency as a funding source for purchases in 2021. For that purpose, cryptocurrency holdings will automatically be converted to fiat currency for users. Users can also utilize a service which lets them link a debit card to their cryptocurrency account. Thus, it will actually be possible to use Bitcoin like a credit card. For that, your financial provider will have to immediately convert your Bitcoins into dollars.

Apart from this, people in countries with relatively unstable currencies occasionally prefer to use cryptocurrency over their own currency. In such situations, Bitcoin offers an opportunity to store value without depending on a currency supported by a government. Thus, in the case of a severe economic crisis, people will have a reliable option to fall back on. This phenomenon can be observed in countries which are in great debt, such as Argentina, Venezuela, and Zimbabwe, where Bitcoin has been gaining significant popularity among people.

However, it is important to mention that if you use Bitcoin as a currency instead of an investment in the US, you must keep certain tax implications in mind as well.

How to buy Bitcoin?



People usually buy Bitcoin using exchanges like [Coinbase](#), [Gemini](#), and [Kraken](#), which allow you to buy, sell, and hold all kinds of cryptocurrency. You will also be able to create a new account, similar to a brokerage account, by verifying your identity and submitting a reliable source of funding, such as a debit card or bank account. You can also purchase Bitcoin at a broker, such as [Robinhood](#).

After buying your Bitcoin, you will also require a digital wallet to store it. There are two different kinds of wallet available – hot wallet and cold wallet. A hot wallet or online wallet is one which is stored in the cloud by an online provider like Mycelium, Electrum, and Exodus. On the other hand, a cold wallet or mobile wallet stores Bitcoin without being connected to the internet. Prominent mobile wallet options are Ledger and Trezor.

There are certain things you need to keep in mind while buying Bitcoin. First of all, although Bitcoin is costly, it is possible to purchase fractional Bitcoin from certain vendors. Secondly, do not underestimate fees. Upon a superficial look, they simply seem to be minor percentages of your total crypto transaction amount. However, they can add up on small-dollar purchases and cumulatively form a huge amount in due course.

You must also remember that unlike a lot of other equity purchases, Bitcoin purchases are not immediate. This is because, as mentioned above, Bitcoin transactions must be verified by Bitcoin miners first. Thus, you may only get to see your Bitcoin purchase in your account after ten or twenty minutes.

How to invest in Bitcoin

It is possible to buy and hold Bitcoin as an investment, similar to a stock. This is now possible in unique retirement accounts known as Bitcoin IRAs as well. That said, the philosophies of people who invest in Bitcoin are generally quite variable. For example, some of them choose to buy and hold for the long term, while others consider selling it following a price rally, and. Some people even like to bet on Bitcoin prices rising or going down. Bitcoin's price has been

observed to go through major price swings over time. For example, in 2020, Bitcoin went as low as \$5,165 and as high as \$28,990. In 2021 — it has jumped to \$50k, which explains the volatility of this currency.

Although people have been using Bitcoin to make purchases in certain locations, it mainly serves as an asset that will be rapidly gaining value for some time. Thus, most people who hold Bitcoin choose to be long-term investors. After all, it is common sense not to sell something that would be worth much more in the future than it is today. It is also possible to invest in a Bitcoin mutual fund by purchasing shares of the Grayscale Bitcoin Trust (GBTC). However, it is presently only open to accredited investors who earn no less than \$200,000, or have a net worth of \$1 million or more.

Thus, most Americans are ineligible to invest in the GBTC. However, diversified Bitcoin investing has been growing much more popular in Canada. For example, in February 2021, we witnessed the emergence of the world's very first Bitcoin exchange-traded fund (ETF) in the form of Purpose Bitcoin ETF (BTCC). Also, the Ontario Securities Commission approved the Evolve Bitcoin ETF (EBIT). If you are an American investor interested in Bitcoin (or a system similar to Bitcoin), you should take a look at blockchain ETFs which invest in the technology that drives cryptocurrencies.

However, it is important to remember that although crypto-based funds do make crypto holdings more diverse and relatively secure, they are still much riskier and charge much more fees than broad-based index funds that have histories of reliable returns. If you are an investor who wishes to earn a lot in a relatively short span of time, you should consider index-based mutual and exchange-traded funds (ETFs).

How to Open a Bitcoin Wallet?



If you want to use it, you have to open a Bitcoin wallet which will help you to store the transactions either sending or receiving Bitcoin from one account to the other. It is similar to a bank account but it is not maintained by the government organization.

If you are about to share the Bitcoin which is done based on their Bitcoin address. With the address, you can send and receive Bitcoin to or from your account. As the address has a number of different characters, try to create a QR code that will be helpful for easy transactions.

Different and secure options to open a Bitcoin wallet

Opening a Bitcoin wallet and using it similar to the online banking process. It is easy to manage transactions online.

You can do it either with a mobile phone or a personal computer. The Bitcoin wallet can be used in three different ways. The ways can be web-based, desktop applications and mobile applications. Using any of these options you can view the transaction that you have received and sent.

A web-based wallet helps you to use from anywhere with your login credentials. There are many web wallets available, before choosing just go through whether that is the safest web to use your transactions. Not every web wallet provides the safest transactions.

The portable and easiest way to start a Bitcoin account and using it is on the smartphone. In both Android and iOS, some Bitcoin provide better transactions with your login credentials from the Bitcoin account. The application is also available for Microsoft as well.

Bitcoin application is also available for computers. If you have a personal computer, then download the wallet application on your PC. Desktop applications are more secure than the other two options. Even if it is less convenient it is more secure for your transactions.

Should I buy Bitcoin or not?

Finally, we have arrived at one of the most important questions related to Bitcoin. When it comes to buying cryptocurrency, a lot of

financial experts support their clients' wishes but do not actively recommend it unless the client is specifically interested in the same. Senior experts have expressed that they are mainly worried about the dire consequences if someone's investment in cryptocurrency fails to do well. People who invest a large part of their life's savings in such a venture may actually end up bankrupt and broke. It is definitely not worth taking such a large risk.

Considering the speculative nature of cryptocurrency, some financial planners suggest that it can be used for clients' side investment, or a "Vegas account". Namely, it should not be used as a part of your long-term goals, or a large part of your portfolio.

Basically, Bitcoin is very much like a single stock, and experts never advise putting a large portion of your portfolio into one company. You should never consider investing more than 1% or 10% into Bitcoin, even if you are extremely interested in it.