

# How to Get Your Virtual Hands on Your Very Own Bitcoin

# The Art of making Bitcoin and other Crypto Currencies

---

Online: [BitcoinGuides.net](http://BitcoinGuides.net)

## Preface

---

The main purpose of this guide is to provide ideas and information on how to safely use Bitcoin and Bitcoin services to avoid many undesirable and harmful effects that others have experienced. Ideas can only be overcome by other ideas. Money and force are impotent against ideas. The abandonment of sound money is the chief reason, if not the only reason, that the world has become such a dangerous place. Bitcoin, being merely open-source software code, is a powerful idea and tool to counteract these evils.

With love from [BitcoinGuides.net](http://BitcoinGuides.net)

# Contents

---

The Art of making Bitcoin and other Crypto Currencies.....	2
Preface .....	2
Introduction to Bitcoin.....	4
How to get your virtual hands on Bitcoin? .....	4
Get free Bitcoin from Bitcoin Faucets.....	4
Make Bitcoin with Your Computer & Graphic Card .....	6
Make Bitcoin with Cloud Mining Providers .....	7
Bitcoin Knowledge .....	9
Wallets .....	9
Online bitcoin wallets .....	9
Desktop wallets.....	9
Mobile wallets.....	10
Ledger USB wallet .....	10
Paper wallets.....	10
Transactions.....	11
Mining.....	12
The Blockchain.....	14
Exchanges .....	15
Trade shares.....	15
Alternative coins .....	15
Buy and Sell Bitcoin & other cryptocurrencies .....	17

# Introduction to Bitcoin

---

Bitcoin is a new currency that was created in 2009 by an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middle men – meaning, no banks. It is created and held electronically. No one controls it. Bitcoins aren't printed, like dollars or euros – they're produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems.

Satoshi Nakamoto is the creator or creators of Bitcoin. It is not clear whether the name is his real name or a pseudonym. He (or she or they) published the Bitcoin paper (Nakamoto, 2008a) in 2008, writing to the metzdowd cryptography mailing list in November 2008 (Nakamoto, 2008). Satoshi initiated the Bitcoin peer-to-peer network and started mining on January 3, 2009.

In today's market Bitcoin is hitting 5000\$ as of 2017 and Forbes Predicts Each

Bitcoin Could Be Worth \$619,047 In 10 Years

[Read more](#)

## How to get your virtual hands on Bitcoin?

---

### Get free Bitcoin from Bitcoin Faucets

A Bitcoin faucet is a website that gives you free fractions of Bitcoin just for visiting. They make income with ads and they pay visitors fractions of Bitcoin called Satoshis, which is also the name of inventor of Bitcoin algorithm. You can withdraw at any time once you have the minimum amount to do a withdrawal.

Visit each of these websites and claim Bitcoins. You can claim many times every day



One of the most popular bitcoin faucets, moonbitcoin. It is one of the most reputable, highest traffic, bitcoin faucets on the internet. The massive traffic allows advertisers to make greater payments for ad space, enabling visitors with more free bitcoin and guaranteed pay-outs.

[Visit MoonBitcoin](#)



I still remember when I discovered FreeBitco.in and was astonished with how well done the site is in comparison to other Bitcoin faucets, how fast the site loaded and after receiving my first pay-out how it has consistently been a reliable source of Bitcoins for me.

[Visit Freebitcoin](#)

## Make Bitcoin with Your Computer & Graphic Card

You can make free Bitcoin with your computer power. This method is now easy, thanks to the new software which allow users easily setup and begin mining with their computers without having trouble to configure programmatically the scripts. You must sign up for one of those websites, install their app and let it run when you want to make bitcoin.

### NiceHash



### MinerGate



NiceHash is a special multi-mining pool MinerGate is a mining pool created by as it allows users to mine any hashing a group of crypto coin enthusiasts. algorithm and to sell the hashing It is the first pool with merged mining. algorithm in the Nicehash hashpower This means that while mining you can exchange to users that want to buy a mine different coins simultaneously profitable mining contract. without decrease of hash rate.

[Visit NiceHash](#)

[Visit MinerGate](#)

[Read full article](#) about how to get free bitcoin and other crypto currencies.

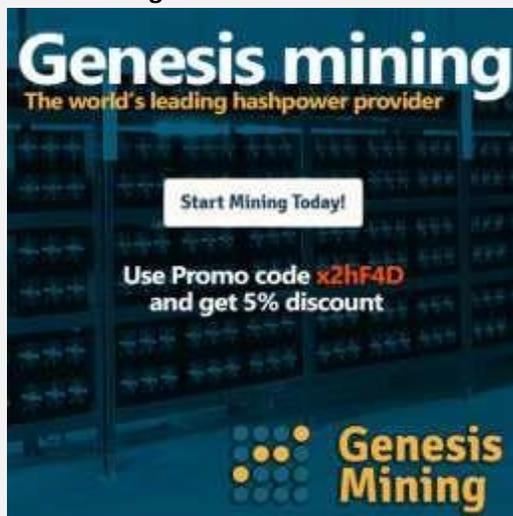
## Make Bitcoin with Cloud Mining Providers

Cloud Mining is a way to mine bitcoin (or different cryptocurrencies) without the need of owning a miner (or mining hardware). Simply said, you buy yourself some shares of mining power – like a mining pool – and profit together with the pool. This means that you only need a contract with someone who offers Cloud Mining Services and a bitcoin wallet.

[Read full review](#) of Bitcoin Cloud Mining Providers

Cloud Mining services are for you if you want to invest in bitcoin mining without the hassle of managing your own hardware, or, in some cases can't invest in high priced ASIC mining hardware. You can use the cloud mining to earn your coins.

### Genesis Mining



Genesis-Mining is the world's leading and most transparent hosted hashpower provider for Bitcoin and Altcoins. Reliable & Customer Oriented. They are heavily

### HashFlare



investing in the best available hardware to stay at the edge of technology.

[Read full review](#)  
[Visit Genesis Mining](#)

Hashflare offers a unique option for mining with a low cost of entry as well as minimal risk and expense, which is opposite to traditional models of mining that involve procurement, maintenance and configuration of highly specialized hardware.

[Read full review](#)

[Visit HashFlare](#)

### Reinvest to multiply

This is so obvious, if you want to get bigger piece of cake, just invest some pennies. Your investment: soldiers working for you. If Every-time you make some small amounts of BTC and you don't really ne Just invest it, you'll get it back later with some profits.

The sweetest part is when you leverage your investments with referrals bonuses. In few months you gold mine working for you on autopilot. Isn't that sweet. So, if you have few pennies or BTC, here are best places to reinvest them



**BTC Clock**

Even if I suspect this site to be a Ponzi scheme (the owners are not transparent enough with who they are) I invested 0.01BTC few months ago and It still paying me back, I've withdrawn my initial investment and reinvested the profit back into it. It still paying, and I think that it will

continue paying for at least the next two years due to Bitcoin prices and traction.

[Visit BTClock](#)

Cloud mining offers a unique option for mining with a low cost of entry as well as minimal risk and expense, which is opposite to traditional models of mining that involve



**Cloud Mining**

procurement, maintenance and configuration of highly specialized hardware.

[View the Best Cloud Mining Providers of 2017](#)

# Bitcoin Knowledge

---

## Wallets

The software that helps a user manage her funds is called a wallet. The functions of the wallet software are to hold (securely) the user's private keys, create transactions that are sent to the network, and collect incoming and outgoing transactions to show the balance of available funds to the user. As a user can own many addresses, most software wallets are ready to manage multiple addresses, aggregating the funds across them.

All wallet software can create new addresses, for instance when it is run for the very first time. To create a new address a key generation algorithm is executed.

Creating a Bitcoin address is straightforward and instantaneous. There are many kinds of Bitcoin wallets:

### Online bitcoin wallets

Web-based wallets store your private keys online. Several such online services are available, and some of them link to mobile and desktop wallets, replicating your addresses between different devices that you own.

- [Coinbase](#)
- [Blockchain](#)

### Desktop wallets

If you have installed the original bitcoin client (Bitcoin Core), then you are running a wallet, but may not even know it. In addition to relaying transactions on the network, this software also enables you to create a bitcoin address for sending and receiving the virtual currency, and to store the private key for it. □

[Bitcoin.org](#)

- [Electrum](#)

## Mobile wallets

Desktop-based wallets are all very well, but they aren't very useful if you are out on the street, trying to pay for something in a physical store. This is where a mobile wallet comes in handy. Running as an app on your smartphone, the wallet can store the private keys for your bitcoin addresses, and enable you to pay for things directly with your phone.

## Ledger USB wallet

Ledger Wallet protects your keys with a secure micro-processor certified against all types of attacks (both physical and logical). This technology has been used in the banking industry for decades (think credit card chips). Our hardware wallet will do all the Bitcoin cryptographic heavy lifting such as signing transactions inside its secure environment. You can therefore use your Bitcoins with maximum trust, even on an insecure or compromised computer. Get yourself one at [ledgerwallet.com](http://ledgerwallet.com)



## Paper wallets

A paper wallet is a document that contains copies of the public and private keys that make up a wallet. Often it will have QR codes, so that you can quickly scan them and add the keys into a software wallet to make a transaction.

Read full tutorial: [Create Bitcoin Digital Paper Wallet – Password Encrypted \(BIP-38\)](#)



## Transactions

Bitcoins do not reside in user's computers. They are entries into a distributed database called the blockchain. Unlike centralized digital currencies, Bitcoin's blockchain does not store accounts and balances. The blockchain stores transactions. Transactions are composed of a list of transaction inputs (TxIn) and a list of transaction outputs (TxOut). Each transaction output (TxOut) holds two pieces of data: an amount and the recipient address. The address is derived from the public key.

Thus, only the owner of the private key can unlock the funds stored in the TxOut. To unlock the funds, the owner of the private key must sign a transaction sending the funds to a new Bitcoin address. A transaction input (TxIn) holds a reference to a previous transaction output, and a signature that proves that the funds in the previous TxOut it references can be spent. This signature must be done with the private key associated with the public key in the Bitcoin address. If the signature does not match, the transaction is deemed invalid and dropped by the network.

A transaction groups several TxIns and TxOuts (at least one of each). The purpose of a transaction is to distribute the funds from the inputs to the outputs. Inputs in a transaction reference outputs in previous transactions. These outputs must not have been spent, otherwise the transaction is invalid.

For the transaction to be valid, the sum of the amounts of the inputs must be greater than or equal to the sum of the amounts of the outputs. The difference between the inputs and the outputs, if there is any, is the fee of the transaction. The transaction fee is collected by the miners that include the transaction in a block.

To spend the funds stored in a transaction output, the spending transaction must be signed with the private key associated with the address where the funds are stored.

## Mining

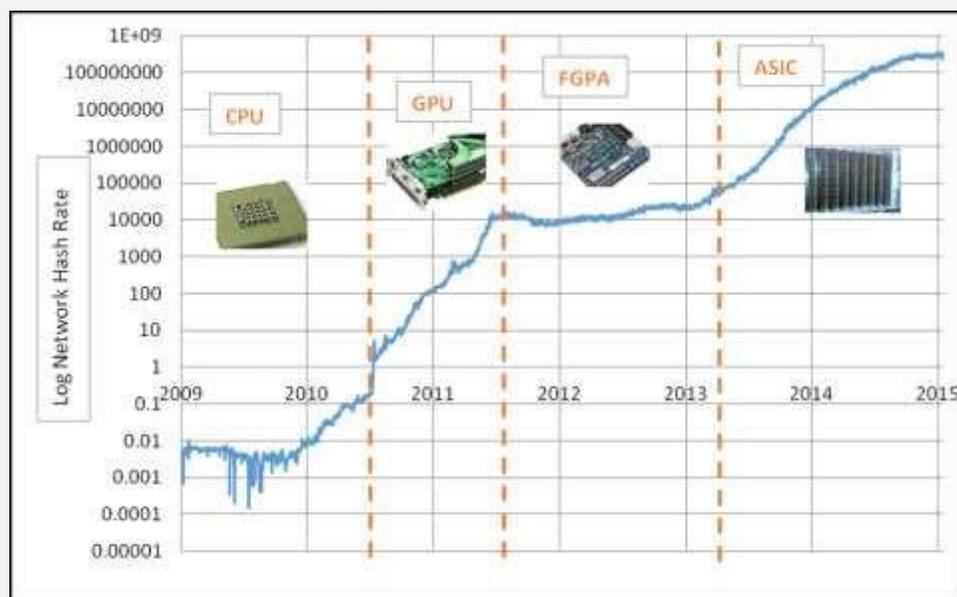
Bitcoin mining was introduced in section 2.1, in the context of the blockchain. Mining is the process of adding blocks to the blockchain. Miners contribute their computational power to solve the blocks that are added to the blockchain, and the network remunerates them with the block reward and the fees collected from all the transactions included in the block.

Miners solve the partial hash inversion problem. To find a solution, mining software usually increments the block nonce and runs the proof-of-work algorithm to check if the chosen nonce generates a correct block hash (i.e. a block hash that meets the difficulty requirements).



One of the advantages of the mining mechanism is that it rewards early adopters for supporting the network. This was very important in the beginning, when Bitcoin bootstrapped itself into relevance. Bitcoin does not have a corporation backing it, so marketing had to be done virally. This would have been impossible without the help of early adopters. Rewarding miners is a way to enlist them to create word of mouth.

Mining hardware has followed a trend toward more specialized hardware where a larger part of the circuitry of the chip is dedicated to the hashing function. There have been four phases in this transition:



(Figure 4)

- **CPUs:** CPU stands for Central Processing Unit: the main chip inside computers and other devices. It is general purpose hardware: its computational power can be applied to many tasks, including mining Bitcoin. The initial release of the Bitcoin Core implemented mining on the

CPU. During the first phase of Bitcoin mining, running from 2009 to the summer of 2010, mining was performed only using CPUs.

- **GPUs:** GPU stands for Graphics Processing Unit: the specialized computer chip originally used for graphic acceleration. There is a trend in computing of using the parallel power of GPUs to perform general computations, known as GPGPU or General-Purpose computing on GPU.
- **FPGAs:** FPGA stands for Field-Programmable Gate Array. FPGAs are chips built of logic blocks that can be programmed and interconnected to perform a task. As the name suggest, FPGAs are designed to be programmable “in the field,” i.e. after shipping. FPGAs were introduced in Bitcoin mining in mid-2011 and for a time competed with GPUs
- **ASICs:** ASIC stands for Application-Specific Integrated Circuit. ASICs are chips built for a specific application, in contrast to CPUs (or, to a lesser degree, GPUs) that accept software running many possible applications. ASIC parts have the logic of the SHA256 function copied as many times as the area of the chip allows, to run as many, hash tries in parallel as possible.

Some of the periods of exponential increase (or even jumps) in the network hash rate have coincided with the introduction of new mining technologies. The latest period—ASICs era—is still in progress at the time of writing. However, as the next ASIC iteration (20nm) catches up with the state-of-the-art in chip manufacturing process, the exponential trend in hash rate is set to level off.

## The Blockchain

At the center of the Bitcoin network is a decentralized ledger that contains the balance of every Bitcoin user. Bitcoin identifies users by large strings of letters and numbers such as “1JPbwArgk7d9KxB7uaXZEArfvK5grCBEwD”. The address is the **public part** of a public–private cryptographic key. The **private part of the key** is under the control of the user.

The blockchain is arguably the most important innovation introduced by Bitcoin. It is the missing link that makes distributed peer-to-peer digital currencies possible.

The blockchain is in essence a distributed database holding all the Bitcoin transactions since the beginning (January 3, 2009) and a method to secure this database. The blockchain keeps a secure list of all the transactions. However, there are relevant questions, such as whether a transaction output is spendable, that the blockchain does not answer directly. Software that uses the blockchain, like mining nodes or wallets, must parse the blockchain to extract the relevant information. This information extracted from the blockchain is usually fed to a database.

The blockchain uses proof-of-work to secure the distributed database.

This means the blockchain is secured against tamper attempts by the computational power that has been applied to create it. An attacker wishing to change the blockchain would have to apply a computational power equivalent to all the computational power spent from that point in time to the present. Furthermore, the attacker would have to outrun the legitimate Bitcoin network, which keeps adding entries to the distributed database. In other words, it would have to catch up, computationally speaking, with the legitimate network to change the information in the database. Attacks to the blockchain will be covered.

The blockchain is an ever-growing chain of blocks. Each block contains a group of new transactions and a link to the previous block in the chain. New transactions in the network are collected into a block which is appended to the blockchain. Note that old transactions are still in the blockchain: old blocks are never removed from the blockchain, thus the blockchain can only increase in length.

The miner who solves the hashing problem uses the coinbase to pay the block reward to herself. Therefore, solving the partial hash inversion problem is called mining. All miners in the network compete to mine blocks. The hash rate of a miner is her computational power, measured in hashes/second. The network hash rate is the total hash rate of all the miners in the network, and it stands at around 30,000 TH/s at the time of writing. Mining a block can be compared to a lottery, where the chances of a single miner are proportional to her share of the network hash rate.

## Exchanges

Exchanges allow users to convert bitcoins (and other cryptocurrencies) to fiat money. Some exchanges allow the conversion of different cryptocurrencies, such as between bitcoin and other alt-coins.

Exchanges admit different types of orders such as limit orders or market orders. The orders are gathered in an order book that is run through an order matching algorithm. Exchanges collect fees from both parties in the trade. Most exchanges operate continuously, on a 24/7 schedule.

## Trade shares

You now know that bitcoins behave like usual shares or currencies. It means you can apply all the powerful methods of technical analysis — that's the collection of tools that was developed for professional traders and have made many of them astonishingly rich. Of course, you need to be smart (and, if you are reading this book, you are!) to outsmart the market and the brave. And, we must add the usual disclaimer: only invest money that you can afford to miss. Never invest borrowed money as you might end in deep trouble otherwise.

What is the idea of technical analysis in a nutshell? —It is very simple. You can gain much more for your investment if you do not just sit and wait, but rather use the cyclic character of price evolution and sell your stock (here bitcoins) when the price is high and buy them again when the price is low. To do it properly, you need to determine the trend and find the right moments when the trend is reversed.

## Alternative coins

Alternative coins or alt-coins are cryptocurrencies that copy many of the features of Bitcoin. Most of the alt-coins are based on Bitcoin's source code with some changes. As Bitcoin's code is released under an open source license it is acceptable to take a copy of the code, modify it, and release a new cryptocurrency. Many developers have done exactly that, creating many alt-coins.

Development in Bitcoin has been conservative and value-preserving, focusing on avoiding the introduction of errors. On the other hand, altcoins often do not have the restrictions of a production system like Bitcoin, or the requirement of backward compatibility, allowing them to test new tweaks and features. However, Bitcoin can opt-in some of these features if the developers consider them worthy.

Some alt-coins that have proposed interesting changes, either technical or to the economics of Bitcoin. The focus of the chapter is to highlight these changes with respect to Bitcoin.

## ETHEREUM

Ethereum is an open source second-generation distributed ledger with an associated Turing-complete platform, which can be used to build and distribute decentralized applications. Ethereum will create its own blockchain. As of the time of writing, the project is still being built, although the test network is up and running.

## LITECOIN

Litecoin (LTC) is arguably the most successful alt-coin. It was released in 2011 and as of the time of writing had a market capitalization of roughly 5% of that of Bitcoin. It is sometimes referred to as “silver to Bitcoin’s gold.”

## PEERCOIN

Peercoin (PPC) was introduced in 2012. Its main innovation is that it uses a hybrid proof-of-stake/proof-of-work system. In a proof-of-stake system new blocks are minted—analogue to mining—by holders of coins in proportion to how many coins they control. Proof-of-stake does not involve solving a partial hash inversion problem and thus requires minimal electricity consumption.

## NAMECOIN

Namecoin (NMC) is both a crypto-currency and a decentralized key/value store. This decentralized key/value store is used to implement an alternative Domain Name System (DNS). The DNS is the piece of the internet infrastructure that enable human-readable addresses to be resolved to IP addresses. Users running a Namecoin node have a full copy of the key/value store and can access it at any time. Or some users might prefer to connect to a Name-coin node and query the node for specific information.

## DOGECOIN

Dogecoin (DOGE) was introduced in 2013. Dogecoin is a straightforward fork of Litecoin. Its main innovation lies in its marketing strategy. It associates with the famous internet doge meme, transmitting a message of light-headedness and fun that will hopefully cater to a wider demographic than other cryptocurrencies.

# Buy and Sell Bitcoin & other cryptocurrencies

---

First thing to consider when looking for the best bitcoin exchange is how safe it is. This boils down to asking: is it a trustworthy exchange providing transparent data of coins in cold storage (more on this later) and are customers happy? It's also good to look out for which currency pairs are available: are you looking to trade bitcoin for USD, Euros, or other fiat currencies. The location usually gives an idea of what's on offer. However, the largest bitcoin sites usually have many options for buying bitcoin with government issued currency and altcoins.

The sheer complexity of researching where to trade bitcoin led me to make this blog. Although you should always do your own research before investing, I hope this helps. Below is the table of the best exchanges to buy bitcoin online. If you are new to cryptocurrency exchanges, then look out for the 'beginner-friendly' column.

There are now many bitcoin exchanges you can choose from, and more flexibility in terms of payment options. Here are the best exchanges you can use to buy and sell bitcoins and other cryptocurrencies.

## QuadrigaCX



[Visit QuadrigaCX](#)

The most convenient way to trade

Bitcoins with the same day funding & withdrawal. When it comes to Volume, QuadrigaCX is the fastest growing Bitcoin Exchange in Canada, and one of the fastest growing exchanges in the world. Our rapidly increasing volume makes it easy to buy or sell Bitcoins at the best rate.

## CoinBase



[Visit Coinbase](#)

[Read full review](#)

One of the most reputable bitcoin exchanges available, Coinbase is popular among fans of the 'dollar cost averaging' method, where users can automate bitcoin purchase every week or month. It is a no-fuss platform for just bitcoin buying and selling.