

**SAM PATTERSON**

# **BITCOIN BEGINNER**



**A STEP-BY-STEP GUIDE TO BUYING,  
SELLING AND INVESTING IN BITCOIN**

## **Table of Contents**

[Introduction](#)

[What is Bitcoin?](#)

[Bitcoin as a Currency](#)

[Bitcoin as a Payment System: Solving the Double Spend Problem](#)

[History of Bitcoin](#)

[Why Use Bitcoin?](#)

[The Advantages and Disadvantages of Digital Money](#)

[How Does Bitcoin Work?](#)

[Public-key Cryptography](#)

[Millions of Deposit Boxes](#)

[Mining for Coins](#)

[A Chain of Blocks](#)

[Network Verification](#)

[How to Obtain Bitcoin](#)

[Digital Faucet: Free Coins](#)

[Sell Your Stuff](#)

[Purchasing Bitcoins](#)

[Storing and Securing Your Bitcoin](#)

[#1 — Bitcoin-Qt: The Real Deal](#)

[#2 — The Modified Clients](#)

[#3 — Accessible Anywhere: Online Wallets](#)

[#4 — Bitcoin on the Go: Mobile Wallets](#)

[#5 — Paper wallet](#)

[The Threats](#)

[Avoiding These Risks](#)

[Spending and Accepting Bitcoin](#)

[Accepting Bitcoin](#)

[The Future of Bitcoin](#)

[Learn More](#)



## Introduction

Throughout history, the primary method of communicating with someone over long distances was sending a letter. This could take days, weeks, even months, with no guarantee the letter would arrive at all. Even then it was only one-way communication, for a conversation to take place it would take longer still.

Email changed communications drastically. Messages were sent and received instantly, from anywhere in the world. Before email, people didn't even recognize the drawbacks of the old communications system. Once email became widely adopted, the drawbacks were instantly obvious, and we've never looked back.

This is true of our current system of money today. Most people don't stop to think about the drawbacks of our current monetary system, but a new technology is already beginning to change that. This new technology—called Bitcoin—is rapidly changing the way we view money.

This guide will explain to you what Bitcoin is, give a layman's view of how it works, and explain exactly how you can obtain Bitcoin, store them safely, spend them, and even create them yourself. Bitcoin is a complicated subject, but in this guide I will give you everything you need to know in order to understand the system and get started.

# What is Bitcoin?

When people say “Bitcoin” they are referring to one of two things.

1. A digital currency.
2. A payment system used for sending and receiving money online.

Typically the term is used to apply to the currency itself, but the payment system is every bit as important as the currency. Let me explain both.

## Bitcoin as a Currency

Bitcoin is a digital, decentralized, peer to peer, pseudonymous currency based on cryptography. If that sentence made no sense to you, don't worry - I'll break it down for you.

**Digital** – Bitcoins exist only as code, they do not exist as anything physical. People can (and have) made physical representations of Bitcoin, but ultimately they are based in the digital world.

**Decentralized** – There is no central bank or institution that issues or controls Bitcoin. It is a group of individuals all over the world who run the program that keeps the monetary system running.

**Peer to Peer** – You control your own Bitcoin, and when you send Bitcoin to someone else, it goes directly to them. There are no banks or middlemen.

**Pseudonymous** – While all Bitcoin transactions are publically viewable in an open ledger called the Blockchain (we'll get to that later), the sender and receiver are only known as a string of numbers and letters. If you're careful about your identity, using Bitcoins can be done anonymously.

**Based on Cryptography** – The strength of Bitcoin as a digital currency lies in the code, which uses strong cryptography to ensure that the coins cannot be accessed without proper permission.

Bitcoin is the first digital currency that has these characteristics, and as a result it is the first digital currency to become widely adopted on the internet. As of June 2013, it is handling nearly 60,000 transactions each day, and this number is accelerating quickly.

## Bitcoin as a Payment System: Solving the Double Spend Problem

As a new digital currency, Bitcoin is impressive, but the truly revolutionary aspect of Bitcoin is in a new payment system. Before I explain this system, let me briefly describe one of the primary reasons why digital currencies have always failed in the past.

In the physical world, money can't be in two places at once: once you spend it, it is inside store A's cash register and it can't be in store B's cash register. With digital currency, this isn't necessarily true. Since digital currency is computer code, the same money could actually reside in multiple places. This is obviously a huge problem, and would lead to rampant fraud.

However, we do transact huge amounts of money digitally today, so how come we don't see more double spending? Well, we have services that take care of the problem, such as PayPal. They review all the transactions to ensure that the same money isn't spent twice.

But there are substantial problems with using a centralized service to deal with the double spend problem. First, they are a single point of failure. This means that if PayPal were to have technical problems – or perhaps if they don't like what you are trying to purchase – then you can't move your money at all. Also, you have to pay them for their service, typically with fees that are 2% or even higher.

Bitcoin's payment system solves the double spend problem, does it without relying on a single point of failure, and requires substantially smaller fees. It does this by using a public ledger called the Blockchain, which I'll discuss in more detail later in the book.

# History of Bitcoin

Where did Bitcoin come from? Even though it is only five years old it already has a unique story.

The idea for Bitcoin came from a developer named Satoshi Nakamoto. That was the name on the [original paper](#) that laid out the technical aspects of the new project – but it was a pseudonym. The real identity of Satoshi Nakamoto is still unknown.

The original paper was written in October 2008. The nine-page paper briefly touches on each of the major aspects of the system that Satoshi envisioned, as well as naming this new “Peer-to-Peer Electronic Cash System” with the moniker that it uses today: Bitcoin.

After the paper was published, Satoshi created the first software program to begin mining (the process of creating Bitcoin). In January 2009, Satoshi mined the first set of Bitcoin, named the Genesis block. Shortly after, he announced the project to a group of cryptography experts, many of whom were a part of the “cypherpunk” movement. Satoshi developed many of the ideas of Bitcoin from previous cypherpunk works. Initially, this group of computer experts approached Bitcoin as an interesting hobby, discussing how the system may or may not work, and how governments may react to it.

It wasn't until the beginning of 2010 that Bitcoin was used for real-world transactions. By this time, a larger community of developers had reviewed the code – along with Satoshi – and released version 0.2, improving the client. The first Bitcoin transaction for a physical good occurred on May 21, 2010, when a Bitcoin user named Laszlo purchased a pizza worth \$25 – for 10,000 Bitcoins! This transaction spawned the famous “Bitcoin Pizza Index,” which continually updates the price of that first pizza (as of the writing of this book, worth over \$1.2 million).

The Bitcoin community slowly grew over 2010. Mt. Gox, the largest Bitcoin exchange, was founded, and made it easier to buy and sell Bitcoin. The price eventually reached parity with the US Dollar in February 2011, and soon after



began rising rapidly.

This rapid rise was primarily a result of increased media attention. Several new sites began covering Bitcoin, and average internet users began buying them. Also, news of “The Silk Road” began to emerge. This hidden website allowed users to buy and sell illegal merchandise – mostly drugs – using Bitcoin for security and anonymity.

This newfound attention, and scrutiny, drove the price higher still, reaching a high point of \$31 in June 2011. But this rapid price increase would soon deflate. The largest exchange, Mt. Gox, had their database compromised by hackers. This led to some large-scale thefts of Bitcoin totaling in the hundreds of thousands of dollars, which shook confidence in the new currency. The price dropped dramatically, and many wrote off Bitcoin as a failure.

But Bitcoin wasn’t finished, and it slowly began to build more users and followers over the next year. By the end of 2012, there were more users than ever before, and more businesses began accepting Bitcoin as payment for goods and services.

2013 was truly the breakthrough year for Bitcoin. Starting the year around \$13, the price began rapidly increasing as Bitcoin received more news coverage than ever before. Well-known internet brands began accepting Bitcoin, such as Wordpress and Reddit. New users came into the market quickly, and because it isn’t easy to obtain new Bitcoins, the demand outstripped supply and prices rose further. By April 10<sup>th</sup>, the price was a staggering \$266 per Bitcoin.

That price soon collapsed when Mt. Gox again had technical problems, this time due to a long lag time for placing orders. New buyers panicked when the price began dropping, and the flood of sell orders dropped the price down to \$55 in a few days.

After this last bubble, the price has slowly increased and remained much more stable. This is likely due to the increased acceptance of Bitcoin from merchants, and the new services that continue to pop up to make obtaining and trading Bitcoin easier.

As of the writing of this book (June 2013), the total number of Bitcoin transactions has nearly reached eighteen million, and the market cap (number of Bitcoins times price) is over \$1 billion. It isn’t known exactly how many people use Bitcoin, but estimates are typically between 100k and 200k, and growing

rapidly.

In absolute numbers, the United States has the most Bitcoin users, but per capita, Scandinavian countries have the most users. The most rapidly growing adopters of Bitcoin are now – at least temporarily – the Chinese, after several reports on Bitcoin hit their mainstream media. Because of the necessity for having a computer and internet infrastructure, we have yet to see developing countries use Bitcoin frequently.

# Why Use Bitcoin?

## The Advantages and Disadvantages of Digital Money

Now you have a general sense for what Bitcoin is, and know about its history. But why use it at all? What is wrong with our current money?

Bitcoin isn't for everyone. It does require some amount of technical knowledge to purchase and use, as well as safely store your coins. It also is a volatile market, with rapid price fluctuations that can wreak havoc for investors. While these problems will lessen with time, they are still a barrier to many.

However, there are significant drawbacks to our current monetary system that make Bitcoin appealing, and it can be summarized in one word: trust.

Reducing the trust needed for transactions was one of the primary drivers for Bitcoin in the first place. As Satoshi's original paper states in his concluding paragraph, "We have proposed a system for electronic transactions without relying on trust."

In order to use money today, you must have a significant amount of trust in multiple institutions.

1. **Banks.** When using banks, you are trusting that they will be able to pay you back when you withdraw your money, and that they will not go bankrupt. As we have seen many times in history, bank runs and financial panics prove that you cannot be certain your money is safe inside a bank.
2. **Central Banks.** The United States has the Federal Reserve, the European Union has the European Central Bank (ECB), Japan has the Bank of Japan; this is repeated the world over. Countries have central banks that control the issuance of their currency. Typically, this currency is not backed by any commodity (such as gold or silver) and therefore is only valuable by law – also called fiat money. We trust that central banks will not create too much fiat money, which results in inflation and higher prices for everybody. Unfortunately, since the financial crisis in 2008, central banks across the world have all printed more fiat money, which

likely means we will face inflation in the future.

3. **Payment Processors.** We trust that when we spend or accept money online, the payment processors will ensure there are no double spends, and that they will not reverse the transaction. We also trust that they will allow us to spend our money as we like, but this isn't always true. Political advocacy group Wikileaks was trying to solicit donations in 2012, but due to pressure from governments payment processors (such as Visa and PayPal) refused to allow donations from their users.

4. **Governments.** Events in Cyprus during March of 2013 show how dangerous governments can be to our currency. Investors in banks had many of their assets confiscated in order to pay for the country's debt problems. Also, governments tend to restrict the types of things that individuals can spend money on, such as drugs, prostitution, gambling, *etc.*

5. **Identity Required.** For banks, payment processors, and government, using currency typically requires being identified. Under the currency system, unless you are using cash in person, you must be identified, which can cause privacy and security problems.

How does Bitcoin reduce the trust necessary in these institutions? I'll walk through each of them again.

1. **Banks.** No banks are needed when using Bitcoin. You manage the currency yourself, and if you take the right precautions you can be sure your Bitcoin are right where you left them.

2. **Central Banks.** Bitcoin are not created by any central institution, and they are created by the network at a predictable and steady rate. No need to worry about inflation.

3. **Payment Processors.** There are none. Bitcoin is peer-to-peer, meaning the transaction occurs directly from one user to another. No middlemen at all.

4. **Governments.** There is little that governments can do to negatively impact Bitcoin. They cannot confiscate coins from banks, and they can't prevent users from spending their Bitcoin however they like. However, they aren't completely powerless: they can target the exchanges, the points at which people buy or sell Bitcoin for fiat currencies. Still, their control

over Bitcoin is substantially less than traditional currencies.

5. **Identity Not Required.** If you choose to be anonymous with Bitcoin, you can be. Even though all transactions are publicly viewable on the blockchain, the sender and receiver of the funds are only known by a string of numbers and letters. If you're careful, you cannot be identified in the blockchain.

Using Bitcoin means not having to place trust in these institutions. While this argument was the primary selling point for Satoshi, there are many other advantages that Bitcoin offers as well.

**Simple to use.** While they may not be very easy to obtain, they are easy to spend. All you need to do is input the receiver's public address (often done by scanning a QR code), enter the amount, and hit send.

**Internet Integrated.** Bitcoin is made for the internet, and it shows. It is very easy to integrate Bitcoin into online services. Many websites offer Application Programming Interface (API) around Bitcoin services such as the current price, or details on the blockchain. One good example is [Bitcointip bot](#) on Reddit, a popular website that aggregates content. This bot allows users to send Bitcoin to each other, within Reddit itself.

**Fast.** A Bitcoin transaction occurs as quickly as sending an email. Wiring money to another country could take days, but only takes seconds with Bitcoin. However, it is wise to wait for verification from the network – I'll talk about that soon.

**Secure.** The cryptography behind Bitcoin is very advanced, and currently it isn't feasible for anyone to break it. Nearly all theft of Bitcoin has occurred because of improper storage of the coins, or a hacking of the exchanges themselves. As far as anyone in the community knows, no one has ever broken the cryptography – and it isn't for lack of trying! Several well known security experts have openly tried to expose security holes in the code, only to admit defeat.

**Deflationary.** There will only be 21 million Bitcoins ever created – we are at 11 million now – and this slow monetary growth means that the coins will likely increase in value over time. While there is no certainty that this increase relative to fiat money will continue, if the coins are in demand and used for transactions as they are today, the price should

continue to slowly rise as fewer and fewer Bitcoin become available.

Because of these advantages, the number of people using Bitcoin has continually grown since its introduction in 2009. However, Bitcoin isn't perfect. Here are some of the disadvantages.

**Steep Learning Curve.** Many people are turned off to Bitcoin before they even try it, due to the complexity of the issue. Learning about cryptography, the blockchain, mining, maintaining wallets, updating software - all of these things intimidate everyone but the most tech-savvy. Fortunately, as Bitcoin becomes more popular more effort is put into explaining Bitcoin in a more accessible way (as this book is doing!).

**Obtaining Bitcoin.** Getting your hands on some coins is still not a simple process. It can take days, or even weeks, to obtain them online. Again, this is changing – new exchanges are opening every month and as more people own Bitcoin themselves they are more able to sell them in person.

**Confirmation Takes Time.** Transactions occur quickly, but to be certain that the rest of the network agrees the transaction is valid, there is a wait for confirmation. For larger transactions, the recommended time is 6 blocks (explained later), and this typically takes an hour. Of course, you don't *have to* wait that long – many users accept zero confirmations.

**Protecting your Wallet.** Just like in real life, if you don't protect your Bitcoin wallet you can have your money stolen. Securing Bitcoin can be somewhat difficult, since any computer connected to the internet is potentially vulnerable. There are ways to secure your coins, but they do require some effort and technical knowledge (I'll walk through them later).

**Limited Acceptance.** The number of merchants accepting Bitcoins is increasing daily, but it is only a small fraction of the overall economy. For online services especially, Bitcoin is gaining credibility and notoriety, but in other sectors it is only now making inroads. It may be many years – if ever – that Bitcoin is accepted as widely as other options such as Visa or PayPal.

**Uncertain Future.** While all signs point to Bitcoin becoming the first true currency of the internet, there are no guarantees. It may completely

crash and burn, leaving hundreds of thousands of users with worthless coins.

Taking all the advantages and disadvantages into account, who is Bitcoin most useful for? Who shouldn't be using it?

Historically, the most typical Bitcoin user was a technically adept young man in his late 20's or early 30's who has libertarian political leanings. The appeal is obvious: Bitcoin appeals to the tech-savvy, it is something new that is interesting, and it has political implications that tend toward less government control over society.

But this profile of a stereotypical Bitcoin user is beginning to break down as more people are interested in Bitcoin purely for its business benefits. The story of Bitcoin in 2013 has been the business interests that are starting to take Bitcoin seriously.

PayPal CEO John Donahoe made headlines when in May he told the Wall Street Journal, "It's a new disruptive technology, so, yeah, we're looking at Bitcoin closely. There may be ways to enable it inside PayPal." Peter Thiel's Founders Fund invested \$2 million in the Bitcoin company BitPay. Fred Wilson of Union Square Ventures – early investor in Twitter and Kickstarter – invested \$5 million in another Bitcoin company, Coinbase. Cameron and Tyler Winklevoss, of Facebook fame, invested heavily in Bitcoin, reported capturing 1% of the entire market.

These investors aren't interested in Bitcoin because they are passionate about cryptography, or because of their political leanings – they recognize that it might be the currency of the internet in the future, and want to be involved in that process.

So, should you use Bitcoin? If you primarily transact business offline, then I wouldn't make the investment now. Wait a few years until the big investors have created a larger infrastructure, and the Bitcoin economy has grown. Then there will be a smaller learning curve, fewer barriers to obtaining coins, and you won't need to understand the technology.

However, if you buy or sell goods or services online, I would familiarize yourself with Bitcoin now. For a seller, an active community of Bitcoin users already exists, and accepting Bitcoin for your services is a low cost way to appeal to an emerging market. As a buyer, transactions are simple, quick, and

don't require any fees or signing up with your personal information. Using Bitcoin online will make you understand why it is dubbed the currency of the internet.

There is a reason to have Bitcoin apart from being a part of the internet economy – investment. There are two primary reasons people invest in Bitcoins.

1. If central banks across the world continue to devalue their currencies, then holding Bitcoin may protect against inflation. Despite the valid concern over inflation, I would caution against significant investment in Bitcoin as an inflation hedge. The currency is still young and needs to prove itself; if we did face a severe economic downturn it is unknown how widely accepted Bitcoin would be.
2. If Bitcoin becomes widely adopted, even replacing some national currencies, then it will become incredibly valuable. Since the supply of Bitcoin will never exceed 21 million, if the demand for coins rises because it is widely used, then the price will necessarily increase as well. Some predict prices in the thousands, or even tens of thousands, per 1.0 BTC. I don't believe it is likely to ever achieve that amount of acceptance. However, the potential upside is significant, so as long as you can afford to lose the investment, it may be a speculation worth making.



# How Does Bitcoin Work?

At this point, you might be interested in learning how you can obtain Bitcoin. I discuss that [here](#), but before you skip to that part, it would be valuable to understand the inner workings of this new technology. It isn't a necessity to know how Bitcoin works in order to use it – so you can skip ahead if you like – but I do recommend that users familiarize themselves with the basics so they aren't completely in the dark when it comes to their own money.

## Public-key Cryptography

To understand Bitcoin, you need to understand the principle of public-key cryptography. While the details are complicated, it essentially means that each user that wishes to communicate with another user has two keys (groups of numbers). One key is public; everyone can see this series of numbers. Another is private; only the individual user has this key.

Here's an example of how public-key cryptography is used. To send a secret letter, Alice would encrypt the letter using the public key of Betty. Alice then sends this letter along. Betty receives the letter, and then decrypts it using her private key.

The reason public-key cryptography is powerful is because it doesn't matter if someone else – let's say Charlie – intercepts the letter. Without the private key that only Betty has, he can't decrypt it. This technology allows everyone to see the encrypted letter, but only the intended recipient can actually read it.

## Millions of Deposit Boxes

How does Bitcoin use public-key cryptography? Earlier I mentioned the blockchain – a public record of all Bitcoin transactions. Think of the blockchain as having millions of safety deposit boxes, made out of bulletproof glass. The boxes have varying amounts of Bitcoin inside them, but are securely locked. Even though everyone can see what each box contains, only the owners can unlock them.

These deposit boxes are called the *public keys* – everyone can see the numbers (also called an address), and the amount within the boxes. The owners of each deposit box access their Bitcoin using their *private key*. While everyone can see the deposit boxes, and the amount of Bitcoin inside, only the owners of the private key can use the money.

In our earlier example, Alice sent Betty a message that only Betty could read. Bitcoin works the same way, except we aren't sending letters but instead information telling your deposit box to give some of your Bitcoin to another deposit box. To use the example again, here's how it works. Alice wants to send 1 BTC to Betty, so she sends out a message to the entire network. This message includes Betty's public address (the location of her deposit box), the amount of Bitcoin she wants to send to Betty, and a digital signature that verifies she is the owner of the private key to her own deposit box.

When Alice sends this message to the network, other network users verify that this message is accurate. If all the numbers match up, then the transaction gets put into a block (a collection of other transactions), and this block eventually gets published in the blockchain. Once that occurs, the rest of the network recognizes that Alice's deposit box is 1.0 BTC smaller than before, and Betty's deposit box has grown by 1.0 BTC. Since the blockchain is a public ledger that extends all the way back to the first Bitcoin transaction, it knows the exact amount of Bitcoin in every deposit box that exists.

## Mining for Coins

Now you understand how transactions take place, but you might be wondering where Bitcoins even come from in the first place. Remember how I mentioned some network users verify the transactions are accurate, and then include them in a block to be published to the entire network? This process requires significant computing power, so why would other users be willing to do this? Because they are rewarded with Bitcoin!

Devoting your computer to processing transactions is called mining. Miners verify transactions, and as they are doing so they are looking for the solution to a mathematical problem. If they are the first to find the answer, the code allows them to publish the block of transactions to the rest of the network. Whoever publishes the block gets a reward, currently set at 25 BTC. This reward halves every few years, so that the amount of Bitcoin never grows too quickly. Also, as more people devote more computing power to the network in order to increase the chance of getting a block reward, the difficulty of mining increases. The code automatically adjusts the difficulty of the mathematical problem so that a new block is mined approximately every 10 minutes.

## A Chain of Blocks

One more important thing to mention about the blocks – they are built on each other in a chain (hence the term blockchain). It is imperative to have a continuous and chronological record of all transactions; this ensures the amounts of each and every deposit box have been accounted for. In order to do this, each block has two additional elements apart from the transactions. One is a much-shortened snapshot of all previous blocks, called a hash. This hash ensures that the blockchain is building on the previous blocks, all the way back to the original block (called the genesis block). The second aspect is the answer to the complicated math problem the miners need to solve. The next block cannot be mined until the problem has been solved, ensuring that blocks are created in chronological order. As of June 2013, there have been more than 238,000 blocks published in the blockchain.

In this way, the Bitcoin ecosystem keeps evolving. Transactions get compiled into new blocks, the blocks are published to the rest of the network in a continuous chain, miners get rewards for their work, and those new Bitcoins are used for transactions, starting the cycle over again.

## Network Verification

How is this system kept in check? After all, Alice could send a message saying that she has 5.0 BTC to send to Betty, even though her deposit box only has 2.0 BTC. There are many ways that dishonest users could attempt to trick the system, but fortunately it's virtually impossible. This is because Bitcoin is a decentralized system where all transactions are public, and require verification from the rest of the network. If Alice tried to send more coins than she had, the recipient would immediately check the balance of the account, recognize this, and reject the transaction. It would never make its way into the block, and the rest of the network would never even see the false transaction. This verification is done in the code of the Bitcoin program itself, so it is nearly instant.

# How to Obtain Bitcoin

So, you're sold on the benefits of having Bitcoin. Great! But how can you get them? There are a variety of methods, some simpler than others, but I'll walk through each of them for you.

Before I talk about how to get coins, here is a warning: it is important to know how to properly store and secure them. Your coins are only as safe as you make them. I'll discuss the different ways to safely handle your Bitcoins in the next section, so make sure you've read that section before going out and buying any.

There are four ways to obtain Bitcoin: receiving them for free, selling your goods and services for them, buying them directly, or mining them.

## Digital Faucet: Free Coins

Yes, you can get free Bitcoins. There are multiple websites that give free coins to get users started (called faucets). However, with the rise in Bitcoin's value many faucets have shut down, and the remaining ones give out miniscule amounts of coins. While they were valuable when Bitcoin was in its infancy, I wouldn't bother spending time with faucets today.



## Sell Your Stuff

You can sell your goods or services to obtain Bitcoin. Some Ebay-like websites only deal in Bitcoin, such as [Bitmit](#). A quick search on Craigslist for the term “Bitcoin” will show many dealers offering the products for coin. Internet forums exist for Bitcoin users to buy and sell their own merchandise, such as Reddit’s [Bitmarket](#). This is a relatively simple way to obtain Bitcoin, if you have anything valuable you don’t mind parting with.

While most items offered for sale by Bitcoin users aren’t very expensive, there are some examples of very large transactions. A Texas family sold their Porsche for 300 BTC recently. A Canadian man put his house on the market for Bitcoin.

## Purchasing Bitcoins

The most common way to obtain Bitcoin is by purchasing them. There are many different avenues to purchase Bitcoin, but two ways are the most common.

One is to purchase Bitcoins locally and in person. This frequently occurs if you know someone with Bitcoin. Avid Bitcoin users are often happy to sell a small amount to other users in order to get them started.

However, you certainly don't need to know a guy in order to buy them locally. A popular website called [LocalBitcoins](#) allows you to search for sellers in your area, and then arrange a meeting to make the transaction. These personal transactions do carry some amount of risk, since you have no guarantee they will send you the coin once you hand over the money (or visa-versa!). However, the website uses a reputational system so that each seller has reviews from previous buyers. In this way, it is in a seller's interest to ensure they don't cheat their clients. The vast majority of users report positive interactions with LocalBitcoins.

The second way to obtain Bitcoin is probably the most common of all: purchase them from an exchange or affiliated payment processor. Exchanges are businesses that will buy and sell Bitcoin for various national currencies, such as dollars, pounds, euro, or yen.

Exchanges have been a critical part of Bitcoin's expansion. Originally, miners were the primary users of Bitcoin, since there wasn't really a marketplace to sell their coins. Once exchanges became popular, coins could be purchased by anyone, no need to have a computer set up to mine coins.

There are many exchanges available. Some of them are primarily useful because they serve a specific region or deal primarily in a certain currency. Here is a list of the most popular ones.

[Mt. Gox](#). This is-by far-the largest exchange for Bitcoin. Mt. Gox was an early entry into the market, and for some time they had nearly 100% market share as a Bitcoin exchange. This has slowly declined over time and is now somewhere near 60%. Mt. Gox is based on Japan, but transacts in dollars, pounds, euros, and yen. They have drawn much criticism from the community for not acting in a professional or timely manner, and causing some turmoil in the Bitcoin markets, but they are still the industry leader by a long shot.

[CampBX](#). This exchange is based in the US and deals in dollars. While Mt. Gox no longer accepts payments through online payment processor Dwolla, CampBX still does.

[BitStamp](#). An exchange located in Europe, dealing with multiple currencies.

[BTC-E](#). A Russian exchange, dealing in multiple currencies and also dealing in cryptocurrencies other than Bitcoin.

[Coinbase](#). This service, established in 2012, operates out of California. It allows you to link your bank account directly to their service, enabling users to buy Bitcoin instantly from their bank account. There is a limit on how many Bitcoin you can buy or sell with their service.

[BitInstant](#). A service similar to Coinbase, except you don't need a bank account. For a fee, you can deposit cash at local stores in the US such as CVS or Wal-Mart, and using a payment processor, you'll receive some Bitcoin minutes later.

This is only a handful of the services out there you can use to obtain Bitcoin.

Despite there being many ways to obtain Bitcoin, it often takes patience to finally have some coin in your wallet. Most of the exchanges require identification in order for them to comply with their nation's laws. The process of verifying identification can take days or even weeks. Mt. Gox is famous for having a queue of people waiting for identification that has stretched into the thousands!

Once you're verified, you then need to fund the exchange. For some time, one of the most popular ways to fund Mt. Gox accounts was Dwolla, an inexpensive online payment processor. However, in May 2013 the US government shut down Mt. Gox's account that used Dwolla, citing incorrect permitting. Now getting funds to the largest exchange requires a wire transfer or using another payment processor.

Dwolla can still be used at CampBX, and a few other places, but it's unclear for how long Dwolla will still be a viable exchange funding method. Given the uncertainty around Dwolla for now, what is the best way to obtain coins?

This depends on your level of patience, acceptance of fees, and desired anonymity. If you are patient, want low fees, and don't mind your coins tied to

your identity, I would suggest using Coinbase. It is simple to set up; you just register an account with an email address, and then link a bank account. You can choose to instantly link the account using your online banking login credentials. As trustworthy as Coinbase is, I would recommend their second option. They make two small deposits into your account, and you verify your account based on entering the correct amount deposited. This process does take several days from start to finish, but there are few fees.

If you are impatient and need Bitcoin today, and you can tolerate higher fees, I would suggest using BitInstant. It lives up to its name – once you fill out a form on their site, you go to a local store that offers money transfer services (there are many), deposit the exact amount requested, and only minutes later the coins are deposited in your wallet. Because you need to fill out your personal information, this method also isn't anonymous.

If you want anonymity, use LocalBitcoin and transact for cash in person. Obviously, be careful doing this. As I mentioned earlier, most users report positive results, but there are some scammers in the Bitcoin community who may literally take your money and run. Look for sellers who have a good reputation online.

Be very wary of individuals selling Bitcoin outside of reputable communities. If anyone wants to use PayPal, especially to buy your Bitcoins, that is a warning sign. PayPal isn't a good idea to buy or sell Bitcoin because transactions are reversible, meaning someone could receive the coins then take back their payment.

Do some quick Google searches of the exchanges and services I suggested, and find out which works best for you. But remember; don't buy until you've read the section on securing your coins.

## **Mining for Bitcoin**

There is one last way to obtain Bitcoin, and that is to mine them. For most readers, I doubt this is a viable option, so you can read this section if you have an interest in learning about mining, but feel free to skip ahead.

As I mentioned earlier, mining Bitcoin means that you are lending your computer power to verifying other user's transactions, while searching for the solution to the mathematical problem. The miner that finds this solution first will publish the next block, and receive a 25BTC reward.

25BTC created approximately every 10 minutes is a lot of money, so it's easy to understand why many people want to be Bitcoin miners.

Here's the bad news: The train has already left the station when it comes to Bitcoin mining. It's very unlikely that anyone who would start today and invest the significant resources of time, computing power, electricity, and money into running a mining rig will recoup that cost for a very, very long time – if ever.

If that's true, then why are there so many miners out there? Because mining used to be very profitable. Previously, miners used the CPUs to run the program that mined coins. After awhile, someone realized that using a GPU (the graphics card), would actually solve the mathematical solution much more quickly. More people began running GPU rigs with multiple video cards. As more people entered the mining market, the chances of anyone getting the block reward dwindled.

Miners worked around this problem by joining mining pools. They contributed their computer power to the pool of miners, and in return if the next block was found by the pool, they divided the block reward amongst everyone participating. This worked well for awhile, although mining pools dealt with new problems such as storage space, and cooling their rigs down.

Then a new development in mining came along: Application Specific Integrated Circuits, or ASICs. These rigs were specifically designed to mine Bitcoin – and that is all they can do! Because they do nothing but mine Bitcoin, they don't require nearly as much energy as a standard mining rig. A rig that uses little power and is orders of magnitude better than the previous technology was a significant step forward for miners, but it came with a price. These new machines are in high demand, and so they are expensive – very expensive. Finding a quality ASIC could easily cost thousands of dollars.

This creates a dilemma for anyone looking to enter into the mining market, because now there are so many other players and such advanced technology that the chances of you actually getting a block reward are very small unless you make a significant investment (both upfront and continuing). You would be far better off taking those thousands of dollars and simply buying the Bitcoin directly!

I don't recommend readers attempt to mine Bitcoin. That is becoming a specialized service taken on by increasing larger players with access to infrastructure. Gone are the days where running the Bitcoin client on your laptop

computer could easily bring in hundreds of Bitcoin.

# Storing and Securing Your Bitcoin

Now you know what Bitcoin are, and how to obtain them. There is only one more thing you need to know before you can begin using Bitcoin: storage and security. This is one of the more daunting aspects about using Bitcoin, because if you make a mistake you could lose your coins permanently. It requires some technical skill, though nothing too complex. This isn't a section you can skip. If you do, you may as well be juggling your key-ring over a sewer grate or leaving your wallet behind in a taxi-cab.

First, let me explain some terminology. When the media discusses Bitcoin, they often say that the coins are kept in wallets, which is true but misleading. The coins are actually in their deposit boxes (their public addresses), and a wallet is simply a service that collects all of a user's deposit boxes into one place. Think of a wallet as your own little bank: you have your own row of deposit boxes, and all the private keys to those boxes as well. When you need to send Bitcoin from any of your public addresses, the wallet has your private key right there for you.

This wallet can be stored in many different places. There are five main ways to keep a wallet.

## #1 — Bitcoin-Qt: The Real Deal

The first option is the original option. This is the computer program (called a client) that the core of developers working on Bitcoin release every so often, with updates to make the system better.

This client downloads the entire blockchain onto your computer. Since this is the record of every Bitcoin transaction ever made, there is a lot of data to store. As of June 2013, the blockchain was about 8Gbs in size.

This standalone program has its advantages.

When you are running the program, you are a node in the network, so you are helping the blockchain stay healthy by verifying transactions.

You are not trusting a third party with your private keys, they are stored locally on your hard drive.

The code is the most reviewed and most secure.

There are some disadvantages as well.

Downloading the entire blockchain takes a very long time (hours or even days depending on your internet connection), and significant hard drive space.

It requires time to sync with the network if you haven't run the program in a while.

If you encrypt your wallet, then forget your passphrase, your coins cannot be retrieved.

You are connected to the internet, increasing the chance that someone could steal your private keys.

You can only access your coins from the computer that has the client.

While Bitcoin-Qt is a solid choice to use as your wallet, I would not recommend it for the first time Bitcoin user. There are better choices. If you do want to use the main client, [visit here](#).



## #2 — The Modified Clients

There are some clients that are also standalone programs, but have some different features from the main Bitcoin-Qt client. Here are a few of the more popular modified clients.

[Multibit](#). This is considered a ‘lightweight’ client, since it doesn’t require downloading the entire blockchain and uses fewer system resources. Setting up and syncing the client is much easier and faster than using Bitcoin-Qt. For first-time users who want a standalone program as their wallet, I recommend Multibit.

[Electrum](#). This client doesn’t download any of the blockchain at all, it connects to a remote server. As such, it is very fast. It also allows users to create a ‘secret seed’ when they first set up the wallet. If your computer ever crashed, you could recover your coins using this system, unlike with the other clients I mention.

[Armory](#). This client is very secure and very feature-rich. There are many neat options for users, such as creating a “cold-storage” wallet for extra security. However, this client has more features than a new user will ever need.

### #3 — Accessible Anywhere: Online Wallets

You don't need to have a standalone program on your computer to use Bitcoin, you can use an online wallet. This is exactly what it sounds like: a website that offers to hold your Bitcoins in an easily-accessible online wallet. This has its advantages.

No syncing necessary, your Bitcoin are instantly available.

It can be accessed in more places than just your computer; all you need is an internet browser.

You can use browser plugins to make using Bitcoin online very simple.

Your coins aren't stored on your hard drive, so if your computer crashes your coins will still be safe online.

However, there are some significant drawbacks to using an online wallet.

You trust a third party with your money. While several online wallets have an excellent reputation, it is still a significant risk to let another party hold your private keys.

As I'll explain soon, if you are connected to the internet you are already vulnerable to malicious attackers who could try to steal your coins. Using an online wallet can make that attack even easier.

The online wallet services themselves can be—and have been—attacked. Several have been shut down because of these attacks.

So should you use an online wallet? I do, for small amounts. It's a simple way to keep a small amount of coins available if I'm going out of town and want to make sure I can access some coins easily. But I would never recommend using an online wallet for large amounts of coins.

Which wallet to use? Mt. Gox and Coinbase have wallets built into their services, and both are fine to use, but my recommendation is [Blockchain](#). This is the most widely used online wallet, and for good reason, it is simple but has an excellent reputation.

## #4 — Bitcoin on the Go: Mobile Wallets

You don't need a computer to use Bitcoin at all—most smartphones are capable of using a wallet app. They aren't able to download much of the blockchain at all, and aren't particularly secure either.

Android has many different wallets available. Check the reviews first to make sure they are legitimate. I use an app simply titled “[Bitcoin Wallet](#).” The iPhone is a little bit trickier—they unfortunately don't allow their apps to use Bitcoin. However, you can get a [limited function wallet](#) for download through their iTunes store.

Should you use a mobile wallet? I would definitely use one, but with the same warning as the online wallet: only in small amounts. It's neat to carry Bitcoin with you wherever you go, and if you ever do happen upon a business that advertises they accept Bitcoin, consider buying something small as a show of support!

## #5 — Paper wallet

Not only do you not need computers to use Bitcoin, you don't need smartphones either. In fact, you can keep Bitcoin on nothing but paper.

First of all, why would you even want to keep your coins on paper? Well, that's simple—paper wallets are, by far, the safest way to store your Bitcoin. If you have large amounts of coins, or you don't want to spend the coins but just save them, then you should consider using a paper wallet.

It doesn't seem to make sense that Bitcoin, a digital currency, would be able to be stored on paper. But remember, the beauty of Bitcoin is in public-key cryptography, and the public ledger (or blockchain). To create a paper wallet, all you need to do is create a new public address and private key, put some Bitcoin in the public address, then print off the private key and store it somewhere safe. To use your Bitcoin later, you can input the private key. Often paper wallet generators create a QR code so that you can simply scan the private key.

While the process is simple enough, it gets more complicated to create a paper wallet in a totally secure way. I'll walk you through creating a secure paper wallet later, but first you need to understand why proper storage is so important.

## The Threats

You now know the different ways to store your coins, but what are you keeping them safe from? There are several threats to your digital money, and being aware of them will help you avoid them as much as you possibly can.

1. **Yourself** You are probably the greatest threat to your own coins. This may sound strange, but it's true, there are many horror stories online of people making mistakes and having lost their Bitcoin. There are two primary mistakes that Bitcoin users make. One is to encrypt a Bitcoin wallet, then forget the password. The second is hard drive damage or other technical error that causes the loss of the private key.

Some of the standalone Bitcoin clients allow you to encrypt your wallet, so that if someone gains access to your computer they cannot get your coins. However, people sometimes set up this encryption, then forget about it—until they want to spend their coins. Then they need the password—oops! They can't remember. And if this happens to you, you're sunk; there is no way to recover those coins. I recommend that if you think encryption is necessary, you *write down your password* and keep it in a safe place. This is obviously true for an online wallet as well, since you need a password to log in.

Since many users store their coins on a local drive, another problem is hard drive failures leading to lost coins. This is a shame, since it is so easily avoidable: all you need to do is create a copy of the wallet file and store it on a USB drive or an online storage system, such as Google Drive or Dropbox. If you do have a backup (you should), I recommend encrypting that copy—just write down the password first!

### 2. **Physical Theft: Roommates and “Friends”**

While this is far from the most dangerous threat most Bitcoiners will face, coins can be stolen just like cash. If you have a paper wallet, or a mobile wallet, or a client on a laptop, a thief could simply walk off with your coins. If they know how to use Bitcoin, and they get access to your wallet, they could transfer your coins to another address they own.

This doesn't seem to happen all too frequently, but when I do hear about it, typically it occurs in college dorms or other settings where people have tech savvy acquaintances. If this concerns you, just keep your wallet encrypted and keep a close eye on it.

**3. Active Attacks: Hacking** There are a few tech-savvy criminals out there who try to steal as many Bitcoin as they can. They typically target exchanges or online wallets where there are lots of users, so individual users typically aren't at risk unless they have coins stored online.

Several exchanges have been hacked in the past few years, leading to various amounts of lost coins. As the Bitcoin community grows, and as the infrastructure grows, it is likely that these types of attacks will become mitigated once bigger companies implement more rigorously tested safety measures. For now, the best approach is to store only small amounts in the exchanges or online wallets.

**4. Passive Attacks: Malware** These are likely an even greater threat than active attacks to the average Bitcoin user, since they target the individual computer that might hold the coins. A passive attack is accomplished with malicious software meant to compromise your computer. These can include things like keyloggers, which record all of your keystrokes and send them to the attacker. Keyloggers are commonly used to obtain passwords, and if an attacker has your passwords they have your Bitcoin.

Alternatively, the malware might be a piece of software that searches your computer for a wallet file, and if it finds one, it sends that file (or just the private keys) along to the attacker.

This type of attack can even come from a browser; if you allow a bad script to run it can wreak havoc, especially with online wallets.

This malware is unfortunately all too easy to contract, especially if you don't have good protection against it and are unsafe in your web browsing.

## Avoiding These Risks

There are some specific measures you can take to avoid these risks. A few of them are simple, but some require technical knowledge and some time commitment. You determine how safe your coins are; if you don't have many coins to protect or you are so rich that you don't care, then you don't need to feel compelled to follow these suggestions.

**1. Have a Clean Operating System** Your operating system (OS) is the type of software you use to run your computer. There are three main OS used today: Windows, Mac OS, and Linux. Malware is most happy running on Windows, so it is the least safe client to run a Bitcoin client on. A Mac isn't a whole lot better, but Linux is significantly safer to use for Bitcoin. If you plan on keeping a significant amount of coins on a computer, I would recommend installing a Linux distribution and learning how to use it. They are free and have nearly all the same features that their expensive counterparts have, besides being safer.

In fact, I would recommend getting an older laptop, wiping the hard drive completely, and installing Linux. Finding an old laptop online, through Ebay or Craigslist, is usually simple and cheap. This gives you the most security, since you are certain the OS is clean and cannot have malware. If you are looking for a good distribution of Linux (there are many kinds of Linux to install), I recommend either Ubuntu or Mint.

**2. Recognize the Internet is Dangerous** The internet is an accident waiting to happen, in terms of Bitcoin safety. Your computer—and coins—have a direct connection with anyone else in the world. You have a few options to mitigate this risk. You can operate offline altogether, by using a paper wallet or offline service (the Armory client allows for this). This is the best option for large amounts of Bitcoin, and it is generally true that the more you are able to do offline, the better. Storing Bitcoin offline is called 'cold storage.'

Or you can carefully work on a computer connected to the internet. Using Linux, you will be somewhat safer, since it isn't as easy for an attacker to directly access you, or contract malware. If you are using Windows, you need to ensure you are up to date on your protective software. I recommend using Microsoft Security Essentials, a free program that gives excellent protection. Also make sure to regularly update your software and run the appropriate scans to make

sure you are clean. Just remember that even if your scans show you are clean, it is possible to have malware on a Window system.

Whenever you are browsing the internet, be careful where you go and what you click on. The same is true for downloading files, and torrents. Malicious software is frequently spread through falsely labeled downloads.

**3. Use 2-Factor Authentication** Online exchanges and wallets nearly all offer a service called 2-factor authentication. This means that when you try to log into your account, or when you try to send Bitcoin, it requires that an outside source verify the requests are genuine and not from a malicious source. Typically, this happens by sending you a text on your smartphone or by requiring you to input an authentication code generated by a program elsewhere.

You should always enable 2-factor authentication. I use the Google Authenticator app on my phone, which I prefer, but there are plenty of other systems like this.

**4. Use Paper Wallets** I've mentioned paper wallets multiple times, and that's because they are the most secure and simplest way to store your coins. To generate a truly secure paper wallet, you need to make sure that your private keys are never on an OS that isn't clean and that they never see the internet. To do that, you need to follow these steps.

1. Find a paper wallet generator that is trustworthy. I would suggest using [Bitaddress](#) to create your wallet.
2. You can print off the paper wallet from Bitaddress above, but this is not truly secure, since the private keys are created by a third party *while connected to the internet*. You need to use their tools while offline. To do this, save the Bitaddress page (as an .htm file).
3. Put the file on a USB drive.
4. Open the file on a clean OS that is *not* connected to the internet—and preferably never has been.
5. Generate a new Bitcoin address using the Bitaddress service.
6. Print off the paper wallet.
7. Delete the file and make sure that there is no electronic record of the



private key remaining on the computer or USB drive.

8. Ensure the printed paper wallet remains secure from theft, fire, flood, bugs, or other damage. If you lose your paper wallet, or is it not readable, you cannot retrieve your Bitcoin! Remember, to use Bitcoin, you must have a private key that corresponds to your public address. A paper wallet—properly created—ensures that the private key only resides on a piece of paper, and no one else can use the coins in that particular public address. That's why if you lose your paper wallet, you lose your private key, and you lose the ability to access your coins too.

9. Send coins to the public address of your paper wallet. You're done!

Now, if you want to use those coins, you import your private keys into whatever wallet you are using. Bitaddress, and most paper wallet generators, generate a QR code that allows for quick recovery of your private key when you need it by scanning the code with a smartphone or webcam.

A quick note on paper wallets: If you do choose to 'withdrawal' from the wallet, make sure you take out all the coin from that wallet at once. A paper wallet that has been used once means it is no longer a paper wallet; you will need to create a new one to be completely secure again.

# Spending and Accepting Bitcoin

You've got your coins, and they are safely stored, but what can you do with them? Since Bitcoin is digital money, any way you currently spend your money could be done with Bitcoin. The only restriction is on the other party being willing to accept them as payment.

While the Bitcoin economy is still young, more and more businesses are accepting this digital currency every day. Even apart from businesses, there is an ecosystem of individuals who are trying to transact as many of their affairs as they can in Bitcoin.

For a list of businesses and websites that accept Bitcoin, [visit here](#). Another good [site is here](#). Here are some of the more popular ways to spend coins.

[Bitmit](#). This platform allows buyers and sellers to list their goods for Bitcoin.

[Coingig](#). Another platform service.

[Craigslist](#). Search for Bitcoin on Cragislist and you'll find people willing to sell for coins.

[rBitmarket](#). A subreddit community for buying and selling goods in Bitcoin.

[BitcoinTalk Forum](#). This forum is full of very active users, and has a section entirely dedicated to buying and selling goods and services in Bitcoin.

[Gyft](#). This is a smartphone app that allows you to purchase gift-cards with Bitcoin. Gyft has rapidly become a convenient way to spend coins at stores that don't accept them directly.

[Bitspend](#). This service allows you to spend your Bitcoin almost anywhere (Amazon is popular). You tell them exactly what you want to purchase, send them the Bitcoin in the corresponding amount, and they make the transaction for a fee. There are several of these services available; Bitspend is currently the most popular.

[Bitcoin Store](#). This site deals with electronics, and has surprisingly low prices. A very popular site.

[Wordpress](#). The largest online blogging platform accepts Bitcoin as payment.

[Reddit](#). This extremely popular content aggregation site takes Bitcoin for its extra services.

[Satoshidice](#). A popular gambling site that lets you send Bitcoin as a bet. It's fun, but please play responsibly!

[OKCupid](#). One of the more respected online dating sites accepts Bitcoin for their paid services.

[NameCheap](#). One of the larger web domain and hosting sites.

[Amagi Metals](#) and [Coinabul](#). These precious metals dealers are well-known and happily accept Bitcoin.

[BitPremier](#). If you're rich, check out this luxury site. They have everything from high-end sports cars to yachts.

[Private Internet Access](#). A Virtual Private Network (VPN) that allows you to connect anonymously to the internet. One of the first to accept Bitcoin.

[Seals With Clubs](#). Great online poker site, only uses Bitcoin.

Betting. There are multiple platforms that allow for betting with Bitcoin. [BetsofBitcoin](#) and [BitBet](#) are two of the best.

Charity. Many charities and political organizations now accept Bitcoin. [Here is a list](#) of some of the more popular ones.

Hidden services. There are many sites that aren't accessible through the regular internet that offer goods and services of questionable legality. The most prominent is called The Silk Road, a marketplace for drugs and other items. I would advise against using these sites. Obviously, you do so at your own risk.

This is only the tip of the iceberg. Search around online and you'll find many opportunities to spend your coins.

## Accepting Bitcoin

Since this is a growing market, don't just look for ways to spend your coins—consider offering your own goods or services for Bitcoin as well! You can use the platforms we mentioned above to do this, but you can also use services created specifically for merchants (one of the best is [BitPay](#)). Here is a [how-to guide](#) for small-businesses who want to accept Bitcoin.

# The Future of Bitcoin

Where is Bitcoin headed? No one knows for sure, but a popular refrain is heard in the Bitcoin community: In ten years, either Bitcoin will be worth nothing, or significantly more than today. I believe this is true.

The idea of digital money that you manage yourself is a powerful one, and in the first four years of this monetary experiment we've seen explosive growth. It's easy to see continued growth in both individual users and businesses that accept coins. If it continues at its current pace, the value of 1.0 BTC will continue to rise compared to other currencies. Eventually, goods and services might be priced in Bitcoin itself, instead of relying on other currencies to judge value. Online shopping might not require entering your credit card information, or signing up for a PayPal account. Your identity wouldn't need to be revealed when purchasing goods, unless you made that choice.

Another aspect of Bitcoin that I haven't discussed is the potential for smart contracts, which use the cryptography inherent in Bitcoin to facilitate more complex transactions, such as escrow services, arbitration, or even estate management. If Bitcoin becomes more popular, these services will likely be implemented in the code (as Satoshi originally intended).

But the future is far from certain. There are three primary threats to Bitcoin that I see on the horizon, that could substantially restrain—or even destroy—this new monetary system.

1. **Technical.** Right now the Bitcoin economy runs fairly smoothly, handling tens of thousands of transactions daily. But what will happen if that hits millions of transactions daily? Can Bitcoin handle the same amount of volume that a major credit card does? There is speculation on both sides of the issue, but no one really knows. If the system isn't able to handle a large amount of transactions, its value is obviously limited.
2. **Governmental.** Because Bitcoin can be used for illegal activities (so can cash), and because the Bitcoin system is inherently difficult to

regulate, governments across the world might decide to limit their citizens' ability to use Bitcoin. If this happens, it will obviously inhibit the Bitcoin economy significantly.

3. **Competition.** Right now, Bitcoin is the clear leader among digital currencies, but it isn't the only one. Several alternative cryptocurrencies have taken the Bitcoin code, altered it, and launched their own currency. Some of the most popular ones include Litecoin, PPCoin, and Ripple. These aren't nearly as valuable as Bitcoin, but it is possible that one day another digital currency could replace Bitcoin if it were significantly better.

If Bitcoin can handle large transactions, avoid government restrictions, and beat the competition, I believe it will become the standard currency of the internet. This monetary experiment has evolved from a nine-page paper written in Fall 2008 to a billion dollar marketplace today, with millions of dollars of investment capital flowing into new start-ups, and new services launched each week.

Only time will tell if Bitcoin will be as revolutionary to our current monetary system as email was to the old system of communications. It's certainly off to a great start, and I hope this guide has helped you to join this grand monetary experiment.

# Learn More

If you want to keep up to date on Bitcoin developments, here are a few resources for you.

[BitcoinTalk.org](http://BitcoinTalk.org). This forum is the primary discussion area online about Bitcoin. If you want to be involved in the community, you should definitely check it out.

[rBitcoin](https://www.reddit.com/r/bitcoin). Very active subreddit dedicated to Bitcoin. My primary source for information on the subject.

[Listen to Bitcoin](http://ListenToBitcoin.com). An amazing website that audibly shows Bitcoin transactions in real-time. A must-visit.

[Bitcoinity Chart](http://BitcoinityChart.com). Real-time chart of Bitcoin price and volume. Useful for traders and Bitcoin addicts.

Journalists, Bloggers and Other Media. There are several journalists and bloggers who cover Bitcoin regularly, along with a [Bitcoin Magazine](http://BitcoinMagazine.com).

- o Max Keiser, broadcaster.
- o Jerry Brito, a scholar at the Mercatus Center at George Mason University.
- o Jeffrey Tucker, owner of Laissez-Faire Books.
- o Timothy B. Lee, journalist at the Washington Post.
- o [The Genesis Block](http://TheGenesisBlock.com). Excellent blog about Bitcoin.

### **Further Reading**

Want to read more about Bitcoin? The ebook you've just read is joined by other best-selling products in their category. Feel free to check them out: [Bitcoin Step By Step](#) — \$ 5.99

[Bitcoin: A Basic Explanation of Everything](#) — \$ 4.99

[Bitcoin Revolution: Ending Tyranny for Fun & Profit](#) — \$ 5.99

[Profiting with Bitcoin](#) — \$ 4.99