Liberty.me

Up and Running with BITCOIN

by Sam Patterson

Liberty.me

UP AND RUNNING WITH BITCOIN

GUIDE 1.0

SAM PATTERSON

This PDF is best viewed using Adobe Reader. If you hare having trouble accessing the hyper-links, copy the footnote URL into your browser.

INTRODUCTION

A new technological and monetary breakthrough has recently captivated members of the tech community, the liberty movement, and the financial sector. This guide will show you how to take part in the Bitcoin phenomenon.

This guide isn't meant to give you an overview of Bitcoin, how it works, and its history, nor to discuss the impacts it will have on society moving forward. Much has been written on these topics, and if you're interested you can find some suggestions for other readings at the end. This guide is meant solely to help you use Bitcoin today.

This guide is written for American Bitcoin users, but most of this applies to international users as well. Let's begin.

STEP ONE: UNDERSTAND SECURITY

As with any currency, there are people who are actively trying to steal users' bitcoins. You don't need to be a computer expert to secure your bitcoins, but you do need to understand exactly what you are trying to

protect and how it can be compromised.

Using Bitcoin requires "public-key cryptography." Don't worry, you don't need to understand what that means, except to know that every Bitcoin user needs one thing: a key pair consisting of a public key and a private key. The public key is an address that you use to send or receive bitcoins, a long string of characters, such as 17GpZr1wkzHQtdvtCuj3V8Em8xd9Rbj7At. Everyone can see the public key and the amount of bitcoins that this key holds.

Every Bitcoin user needs one thing: a key pair consisting of a public key and a private key.

Ownership of bitcoins actually means ownership of the private key.

The private key is another string of characters, but this one isn't public. The user controlling the private key that matches the public address controls the funds within that public address. You can't send bitcoins without the private key; this means that *ownership of bitcoins actually means ownership of the private key.*

Now you know what Bitcoin security is all about: protecting the private key! If it's stolen, there's no way to prevent someone from moving your coins to a new account with a new private key, and those coins will then be completely out of your control.

DEFINITION: Wallet. A "wallet" is a program that keeps track of your public and private keys for you. It makes it simple for the user to send and receive bitcoins without worrying about the details.

The private key (and the wallet that contains it) is just a long string of characters, so how do you keep it safe? Here are some general rules. You don't need to follow them all to the letter in order to use Bitcoin, but the more you adhere to these principles the more secure your coins will be.

Back Up Your Wallet

Make sure you never have a single point of failure.

This is first on the list because it is the most important. Since your private key is a piece of data like anything else, if you lose the data your coins are gone forever. There are dozens of stories about people who lost all their coins when their hard drives crashed. This is needless; it is very simple to back up your wallets in case they are lost or damaged. Most wallet software has an option to back up; I recommend putting an encrypted backup (see "Use Encryption Wisely," below) on at least one USB drive, or in a Dropbox account. Alternatively, you can create a paper wallet, which I'll discuss later. Just make sure you never have a single point of failure.

Don't Trust Third Parties with Your Wallet

This seems obvious, but there are many online services that offer to keep your bitcoins for you. You must be extremely cautious in trusting a third party with your bitcoins, because they have the power to take them at any moment and they also could be hacked at any time. Only use the most trusted organizations, such as Coinbase or Blockchain.info (both described in more detail below), and even then I recommend only using them temporarily before you move the coins to your own wallet.

Minimize Exposure to the Internet

Most Bitcoin wallets are stolen via the Internet. There are various ways this can occur, but the safest way to protect against wallet theft is simply to ensure the private keys aren't "hot," meaning connected to the Internet. A cold wallet is either on a laptop that isn't connected to the Internet, on a USB stick, or even printed out on paper.

The safest way to protect against wallet theft is simply to ensure the private keys aren't "hot," meaning connected to the Internet.

Be a Smart Online User

Don't click links in strange emails, don't visit shady-looking websites, don't download torrents indiscriminately, and don't let other people who use your computer do these things. Malicious websites and downloaded material can contain malware that will take your wallet and send it along to someone who will empty it immediately. If you're not sure about a website, use **NoScript**[1] to prevent scripts from running.

Use Two-Factor Authentication

If you do use online wallets, you must use two-factor authentication. This means that in order to access your account, the website requires more than just a password. It will ask for a code that is generated on another device, often a smartphone. This is essential because it prevents someone from accessing your account with just your password, which happens all too frequently. When you enable two-factor authentication on your account, you will be able to choose what your second method of verification is. The most common choices are having a code sent to your smartphone via text message, or using an Android app such as Google Authenticator or Authy.

[1] http://noscript.net/

Use Encryption Wisely

Encryption is a way to make data unusable to anyone other than yourself or an authorized party. Bitcoin wallets should be encrypted when possible, but there's an important caveat. Encryption requires using a password, which presents its own challenges. If you use a password that is weak, you're almost better off not even using a password. There are many articles online that talk about what makes a good password, so I won't cover that here except to say that longer is better.

The other threat from using a password is forgetting it. If you do, your bitcoins are gone forever. Even though it seems counter-intuitive, I recommend always writing down your passwords and keeping them in a secured place in case you need them later. Even better, use a password-management tool such as KeePassX or LastPass.

Go the Extra Mile: Use a Clean Operating System

This is probably one of the best ways to ensure wallet safety, but it requires some effort and being tech-savvy. Your operating system (OS) is an important element in the security of your data. Windows and Mac OS are both very popular operating systems, and as such they are frequently the subject of attacks. Malware is most common on Windows machines, but Macs are targeted as well.

If you want the most security, Linux is the best choice. Because Linux isn't as popular as the other operating systems, malware typically doesn't target it, and the actual design of the OS makes Linux very difficult to target anyway.

There are many different types of Linux operating systems, called distributions. They're free to install. Many users recommend Ubuntu; I prefer Mint myself.

To be clear, it isn't necessary to use a Linux OS for Bitcoin; this is for users who want to go the extra mile for Bitcoin security.

STEP TWO: CHOOSE YOUR WALLET

Now you know how to keep your bitcoins safe, but where exactly do you keep them? Bitcoins are stored in software called wallets, and developers have created programs—called clients—that offer different types of wallets. They vary in their features and security, so I'll mention the most popular ones and let you decide which works for you. If you visit their websites, they have guides to walk you through setting up the wallets.

Bitcoin-Qt

Bitcoin-Qt[2] is the main code and client that keeps the Bitcoin network alive. Using this client helps out the Bitcoin network by acting as a node verifying other transactions. However, to do this, Bitcoin-Qt requires downloading the entire blockchain, which is currently approaching fourteen gigabytes of data and takes hours or days to download. Bitcoin-Qt offers many features, but these are valuable mostly for advanced users. For this reason, I don't recommend new users try the Bitcoin-Qt client.

Definition: Blockchain. The blockchain is a ledger, distributed across thousands of computers, that contains the history of all Bitcoin transactions that have ever occurred. This record is necessary to keep track of who owns which bitcoin.

Multibit

Multibit[3] is a client that only downloads a small part of the blockchain, making it much lighter and faster than Bitcoin-Qt. It's a simple interface that is good for beginners. If you want a simple stand-alone client (meaning it just runs on a local computer), this is a great start.

Electrum

Electrum[4] has a great feature that makes it one of the favorites for new users: it generates a random string of twelve words, called a seed, when you first run the client. This seed is then securely stored on Electrum's servers, and if you ever have your computer lost, stolen, or damaged, you can still recover your coins by getting a new copy of Electrum and entering the seed (which you've stored yourself). This client is also unique because it doesn't download any of the blockchain at all; it is all done using Electrum's servers, meaning this is the fastest and lightest of all the clients I describe here.

However, using Electrum does mean you are dependent on their servers working—although, even if they go down, your coins are still safe; you just won't be able to use the Electrum client. For new users, Electrum is one of the most popular clients.

[2] https://bitcoin.org/en/download
[3] https://multibit.org
[4] https://electrum.org

Armory

Armory,[5] as the name implies, is a very secure and feature-rich client. If you're looking for security over all else, this is the best client. It also has a built-in paper-wallet generator and a neat feature that allows you to create a wallet for an offline computer as well. If you have some technical savvy, and are looking to store large amounts of bitcoins, this is your client. As with the Bitcoin-Qt client, it's not recommended for new users.

Smartphone Wallets

Bitcoin is the currency of the Internet, and the Internet is increasingly becoming a mobile phenomenon. So far the clients I've discussed are standalone clients, meaning they run only on a laptop or desktop computer. However, Bitcoin wallets exist on mobile devices as well.

Bitcoin is the currency of the Internet, and the Internet is increasingly becoming a mobile phenomenon.

A word of caution: Mobile devices are often less secure than traditional computers (and are more easily physically stolen), so I don't recommend keeping a large amount of bitcoins in them. A general rule of thumb is to treat a mobile wallet like a physical wallet: how much cash do you keep in your wallet at any time?

A general rule of thumb is to treat a mobile wallet like a physical wallet: how much cash do you keep in your wallet at any time?

Apple has unfortunately taken a hard stance against Bitcoin wallets on the iPhone and recently shut down the last one available. (There are currently attempts, including the CoinPunk project, to create a wallet that uses only HTML5, meaning it could be used on an iPhone despite Apple's aversion to Bitcoin apps.)

Android is quite the opposite. There are dozens of Android wallet apps to choose from. I use one called Bitcoin Wallet; it's very simple, with a nice interface. Other popular Android wallets include Blockchain.info, and MyCelium.

Online Wallets

There are many online services that offer to keep your bitcoins for you. As I mentioned earlier, I would avoid these as much as possible. For short periods of time, or small amounts of coins, you're probably fine; but keeping a large amount of bitcoins online is not wise.

[5] https://bitcoinarmory.com

There are only a few services online that I recommend. The best is **Blockchain.info**,[6] which has been around a long time in the community and has a good reputation.

Another is **Coinbase**,[7] which—in addition to being a wallet—is also a service to purchase bitcoins.

There's another wallet that isn't quite stand-alone and isn't online either. The Kryptokit wallet is actually a browser plugin for Chrome, as well as a secure messaging platform and news aggregator. This is a new addition to the Bitcoin wallet space, and it remains to be seen how secure and how popular browser wallets will be, but initial reactions are positive.

The Dark Wallet project is trying to do something similar, using a web wallet to mix users' transactions together, making Bitcoin more anonymous.

Paper Wallets

You wouldn't think that the currency of the Internet could be stored on something as archaic as paper, but you'd be wrong. Because your private key is just a string of characters, it can easily be printed off and stored. In fact, paper wallets—if created correctly—are the most secure way to store bitcoins for the long term. Since the private key is necessary to send bitcoins, if it only exists on paper then there is literally no way for those coins to be spent until the private key is changed back into electronic format.

Because your private key is just a string of characters, it can easily be printed off and stored.

Of course there are risks with paper wallets as well. If they are destroyed, your coins are lost; and paper isn't the hardiest of materials. Fires, floods, theft, moisture, and just plain forgetfulness mean that paper wallets should—at the very least—be in multiple safe locations. I personally use paper wallets for my long-term storage, but I also keep an encrypted backup on a USB drive, and have duplicates of both at another location. This level of security is really only necessary for long-term storage of a decent amount of coins.

The Armory client has a paper-wallet generator built in, but you can still create a paper wallet relatively easily without using Armory. Sites like Bitaddress.org create a new wallet for you automatically, and even create it in a layout that is simple to print and store. However, when creating a paper wallet, it's important to make sure you aren't connected to the Internet, where the keys could be visible. There are many tutorials on how to do this correctly. You can **view this video**[8] or you can check out **my book**[9] for more details.

[6] https://blockchain.info/wallet/
[7] https://coinbase.com
[8] http://youtu.be/I1uefzJJ6nM
[9] http://amazon.com/Bitcoin-Beginner-Selling-Investing-Bitcoins-ebook/dp/B00DKLZLB4

STEP THREE: OBTAIN BITCOINS

Now that you know how to secure your bitcoins, and you've selected a wallet (or a few different ones) to store them in, you're ready to get some coins. There are three main methods to acquire them. You can purchase bitcoins, sell your goods or services in exchange for them, or create them in a process called mining.

Purchase Bitcoins

Purchasing bitcoins is the most common way to obtain them. There are many different ways to buy them, but I'll give you a few of the most common.

The first is the simplest, and it's a way that many people get started: buy them from a friend! Most bitcoiners are happy to sell (and sometimes just give away) small amounts of their coins to friends. If you know someone who has bitcoins, ask if you can buy a few bucks' worth to get started.

If you don't have friends with bitcoins, you can find some by attending **local meetups**.[10] There are currently over 350 meetup groups dedicated to Bitcoin in fifty-four countries.

Another way to purchase bitcoins in person is to use a service called **Local Bitcoins**.[11] Here you can find people in your area looking to sell coins for cash. They typically add a fee of about 3%–5% over what you could buy on an exchange. You contact the seller through the site, then arrange a place and time to meet and buy the coins. While most users report great experiences with Local Bitcoins, there are some scammers and thieves out there, so be careful and treat it as you would a Craigslist deal.

If you don't care to buy bitcoins from an individual, there are services that allow you to purchase online. These hubs for buying and selling bitcoins are called exchanges. There are many exchanges, but only a handful that deal in USD and are large enough to mention: Bitstamp, BTC-e, Bitfinex, Kraken, and Vault of Satoshi.

Mt. Gox was the largest Bitcoin exchanges for years, but in early 2014 they folded due to serious technical flaws in their system.

Coinbase is easily the best way to obtain bitcoins online in the United States.

To use these exchanges, buyers set up an account. This usually requires giving out personal information, and sometimes banking information. While most of the exchanges listed above have a good track record (unlike Mt. Gox), using these exchanges does come with some risk. Also, sending money to these exchanges, most of which aren't in the United States, can be difficult.

There's a better alternative. **Coinbase**[12] is easily the best way to obtain bitcoins online in the United States. They are based in the United States, and have an excellent reputation in the community. Once you set up an account with Coinbase, you link the account to

[10] http://bitcoin.meetup.com
[11] https://localbitcoins.com
[12] https://coinbase.com

your bank account. This process typically takes a week or so, but once it's done it's trivially simple to purchase bitcoins directly from your bank account.

Coinbase also allows you to set up recurring purchases, so instead of watching the bitcoin price, you can just buy $20 worth every week and not worry about volatility of the market.

Some users prefer buying bitcoins in person to avoid the fact that using Coinbase or an exchange ties your identity to your coins. However, if this identity question doesn't bother you, I highly recommend using Coinbase as the primary way to purchase bitcoins.

Sell Goods or Services

Another way to get some bitcoins without laying out any cash is to provide goods or services in exchange for coins. There are several Amazon-like sites that allow you to list items for bitcoins, such as Coingig and Crypto-thrift. Several sites allow you to offer up your skills for small jobs, or even full-time jobs to be paid in bitcoins, such as this **subreddit**,[13] Bitgigs, and Coinality.

Create Bitcoins (Mining)

The people who work to secure the Bitcoin network are called miners. They run software that works to maintain the distributed ledger (the blockchain) that makes Bitcoin work. To incentivize this process, the miners receive a payout for their effort, currently 25 bitcoins (to only one miner, or pool of miners) every ten minutes for finding the answer to a certain problem that requires lots of computing power.

Twenty-five bitcoins is a decent chunk of change, so why doesn't everyone in the network mine bitcoins? Because the algorithm that determines how difficult it is to create new coins automatically gets harder as more people try to mine. As new, more advanced devices joined the Bitcoin network (called ASICs), the difficulty went through the roof, and average bitcoiners can no longer make money mining. If you want to make a profit from mining bitcoins, you need to be able to purchase thousands of dollars of equipment and electricity to run the machines. Most folks are far better off buying the same amount of bitcoins directly.

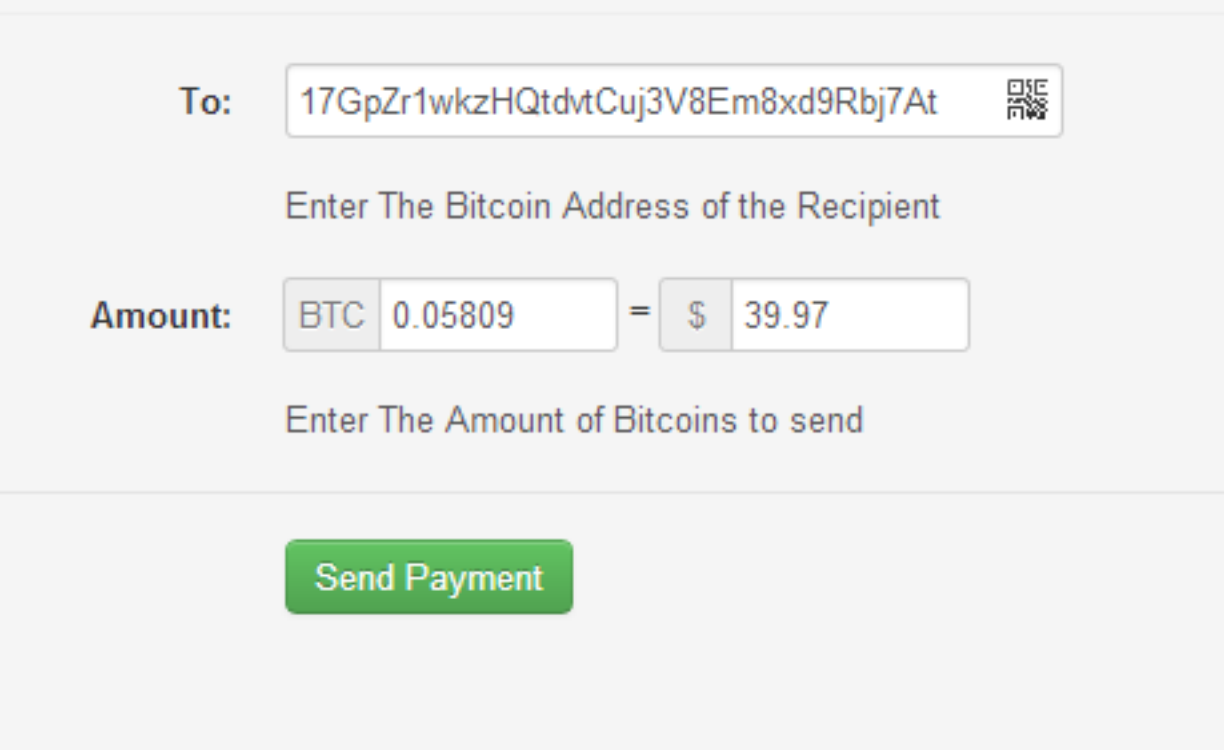
If you want to make a profit from mining bitcoins, you need to be able to purchase thousands of dollars of equipment and electricity to run the machines.

[13] http://www.reddit.com/r/Jobs4bitcoins

STEP FOUR: SEND AND RECEIVE

Congratulations, you've now got the money of the Internet! But how do you use it? Getting bitcoins is the hard part, but using them is simple.

All wallets are different, but they have the same core functions. To send bitcoins, you have to put in the public address of the recipient (a long string of characters) along with the amount you want to send. As an example, here is the interface from Blockchain.info:



You hit send, and it will arrive there as quickly as an email. The same is true in reverse: if you want to get paid in bitcoins, you offer up your public address to the sender.

Since these public addresses are a bit unwieldy, a better method is frequently used, especially for smartphones. QR codes put the address and amount into a picture, which can be scanned by a phone and automatically entered into the wallet software. All you need to do is press send. If you've got a smartphone wallet, you can try it out with the QR code on this page (this one sends a small donation to **Sean's Outpost**,[14] a homeless-outreach project in Pensacola, but you can hit cancel to prevent sending any bitcoins).

QR codes are especially helpful for merchants, either in person or for online shopping.

[14] http://seansoutpost.com/

Where are some places to spend your bitcoins? There are tens of thousands of merchants that accept bitcoins today. You can find a **great directory**[15] at BitPay, a company that helps merchants accept bitcoins. Coinmap also has thousands of listings all over the world. At the beginning of 2014, the large online retailers Overstock and Tiger Direct began accepting bitcoins.

Bitcoins are also used to tip authors, artists, and activists who do something that people appreciate. If you find a Liberty.me author you really appreciate, consider sending him or her a small tip.

Crowdfunding and charity are other common uses for bitcoins. **Bitcoin not Bombs**[16] and **Sean's Outpost**[17] are frequent recipients of bitcoiners' generosity, and it's becoming more common to see a Bitcoin option to donate to projects hosted on Indiegogo and Kickstarter.

LEARN MORE

There are many places you can go to learn more about Bitcoin. Bitcointalk.org is the main forum online, and **this subreddit**[18] is very active as well. Coindesk.com is a news service that focuses on Bitcoin and cryptocurrencies.

You can always reach out to me with questions or comments at **http://patterson.liberty.me**. Enjoy your adventures in the new world of Bitcoin!

Sam Patterson

Sam Patterson is an author and tech enthusiast living in Virginia. He focuses on technologies that have the potential to drastically improve the human condition, such as Bitcoin.

[15] https://bitpay.com/directory#/
[16] http://bitcoinnotbombs.com/organizations/
[17] http://seansoutpost.com/
[18] http://reddit.com/r/Bitcoin/

This guide is published by **Liberty.me**, an online city for friendship, learning, publishing, and sharing practical ways to live a freer life. **If you haven't already, join us today.**

more at Liberty.me