

# **Using Monero**

**A Key Aspect to Our Parallel National Economy**

John Young

Copyright 2020 European Americans United

# Table of Contents

Introduction.....	4
Whence Cometh Monero?.....	7
Word to the Wise on Speculation.....	12
Safeguarding Your Privacy.....	15
How Cryptocurrency Works.....	18
What Makes Monero Better.....	21
Installing Your Monero Wallet.....	23
Installing the Software.....	23
Setting up Your Wallet.....	28
How to Send and Receive Monero.....	32
Receiving Monero.....	32
Sending Monero.....	34
Taking Monero With You.....	37
Exchanges and Coin Swaps.....	39
Obtaining Monero.....	41
Bypassing the System: Local Monero and Bisq.....	44
Bisq.....	44
Keeping Things Honest.....	45
Disadvantages of Bisq.....	47
Let's Buy Some Bitcoins!.....	48
Keeping it Local: LocalMonero.....	48
Internet Resources.....	49
Conclusion.....	50

# Introduction

Let's cut to the chase: the 2020's are going to be a wild ride. They are going to see Texas swing Blue, whereupon only Democrats will be able to win the presidency. Deaths will continue to outpace births for European Americans, and our 56% share of the population will continue to dwindle. The "coalition of the ascendant" that the Left has assembled (with no small amount of aid from the establishment "Right") will continue to demand various benefits, recompense and set-asides at the expense of European Americans, and it will be impossible for politicians to tell them no.

There is only one national group against whom it is not only legal to discriminate, but incentivized: us.

If you look at African-Americans, Jewish-Americans and Mestizo-Americans, it is very rare for one with an IQ over 115 to be under-employed. Nay, the world is their oyster: college scholarships, plum appointments, top 5% jobs. In fact, in the United States, it is only among European Americans where you will find people with an IQ over 115 under-employed, under-educated and bereft of opportunity.

The censorship we complain about now will look like child's play, as "hate" becomes outright criminalized, and websites you take for granted, such as Western Voices World News get shut down. You'll have to find us and other dissident voices on the Onion network, which can't be censored.

And that situation will only get worse as the decade progresses.

On the other side of the equation, we will continue to see government's unfunded liabilities mount, demand for social services increase, and the bill come due as baby boomers slip into retirement and the tax base erodes. There will be a perfect storm of competing ethnic groups combined with resource scarcity, with those at the top considering themselves isolated from the disaster they have spent a century orchestrating. Rather than owning their own shit, you can expect them to "double down" and continue pointing the finger at people like us.

One of the most popular books of the last century was Ayn Rand's "Atlas Shrugged." Rand's emphasis on selfishness as a virtue – a view she shared with the founder of the Satanic church – is based on a purely materialistic worldview that is intensely dehumanizing. Her popularity can be seen, though, in her recognition and naming of numerous problems of the Left – such as the hatred of the good for being good. Likewise, her recognition that some people are indeed more capable than others, and that they ought not be enslaved by those less capable made her a sort of prophet for highly capable people who had been misused.

But her greatest contribution was a what-if fantasy: what would happen if the great minds of the country simply dropped out, went on strike, and started their own thing? This fantasy has captured imaginations for decades, although it has long been technologically impossible. This fantasy has been so attractive because it appeals to what most of us really want: to be left the hell alone so we can have life and liberty while we pursue happiness in what Greg Johnson calls a "nice, white country."

Although physical separation is unlikely to be successful in the near term, quite ironically a successful model for this was established under the repressive regime of the USSR: parallel societies and parallel economies.

We already live under a certain degree of oppression, and that's going to ratchet up over the next decade until matters likely explode in the 2030's. When the USSR imploded, the necessities of life were still there because over the decades parallel economies, societies and supply lines had been established.

Although these parallel systems were often criminal in nature, it's important to keep in mind that it was the USSR who defined them as criminal, because any government will define anything that impinges the prerogatives it arrogates to itself as criminal. Is it immoral to get medicine for a sick person who would die if the law were followed? Likewise, these parallel systems had tightly knit activists for their own racial subgroup at their core. That is to say, their core was composed from a subset of Jews.

Even though the USSR was originally established by Jewish activists and funding, by the mid 1970's the Eastern Bloc had become rather hostile to Jews and Jewish interests. In fact, the origin of so-called "neo conservatism" was among Jewish Leftists in the United States who were opposed to the USSR due to the oppression Jews were experiencing under that regime.

But don't get all tied up in the Jewish thing, because that is not my point. My point is that the core of these parallel networks was formed by a subset of committed members of an ethnic minority. This is what allowed it to be so successful that when the USSR fell, almost overnight they owned almost everything of importance. The primary beef that the U.S. government has with Putin is that he stripped so many of them of those holdings once he came to power, because they misused those holdings to the detriment of majority Russians.

We – ethnically conscious European Americans – are a committed ethnic minority. We are not simply "white people." You and I both know that because of what we know and believe, we have more in common with each other, more trust in each other, than we do the average white person on the street. We are the ideal population to set up a parallel society, economy and supply chain. By doing this, we will be ideally positioned for the opportunities that will await us when matters become less stable.

And this isn't just a pie-in-the-sky idea. It is something that, increasingly, will become necessary for our very survival. What will happen if a President Kamala Harris orders the scraping of the past decade of Facebook posts to identify anyone with pro-European-American sympathies? We have dozens if not hundreds of our people who are already completely unemployable due to investigative "journalists" hunting them down and publicly outing them. What will happen if the power of government gets put behind that effort?

There are many things we need to be doing to be ready for this, or that I have discussed elsewhere. These include an emphasis on developing and honing vital skills, becoming more adept at using "overlay" networks for the alternative (and uncensored) Internet, and much more. This handbook will focus on a very small but vital subset of all of this: simple nuts-and-bolts use of Monero (XMR) cryptocurrency.

Monero has been chosen because it is effectively untraceable. For two years now, it has been the only currency EAU will accept for donations, because it is the only currency that protects the privacy of the donor. But this is also a hurdle because so few people understand cryptocurrency in general, or Monero particularly.

This book intends to remedy that because untraceable cryptocurrency is how a far-flung network of ethnic activists starts organizing a parallel economy.

## Whence Cometh Monero?

Understanding Monero requires an understanding of the social and political context from which it emerged. This is because truly understanding what is going on, and the problems Monero is intended to solve, requires historical context.

The Liberty Dollar and eGold were intended to solve some problems with our existing monetary system. Both were oriented toward solving problems inherent in the Federal Reserve System, and eGold was additionally oriented toward solving problems of privacy.

Any explanation of why alternative currencies would be beneficial has to start with at least a basic understanding of our Federal Reserve System. This is the sort of subject that tends to put people to sleep, so I will just hit the high spots and list some books you can read in the bibliography if you want to know more.

The U.S. Constitution gives the Congress the power to coin money, and explicitly prohibits the States from making anything but gold and silver legal tender. Thus, many people are surprised to learn that the Federal Reserve, despite its name, is neither part of our Federal government, nor is it a reserve. Although the ostensible purpose of the Federal Reserve is to “regulate the money supply” in an apolitical way, in practice it becomes the owner of the country.

Although it is done in a fairly indirect way, this is how the scheme works, and I will explain it in the case of what the Fed calls “quantitative easing.” Pretend you take out a mortgage for \$200,000 to buy a house at 6% interest. Over the course of 30 years, you will pay the bank \$387,000. So they have made \$187,000. But where did they get the \$200,000 to lend you in the first place?

That money could have come from many places, such as by selling GNMA bonds, or from Freddie Mac and numerous other investors. But ultimately, what “quantitative easing” means is that the Federal Reserve itself “bought” the notes for those mortgages, and gave the banks the money. The Federal Reserve literally printed that money out of thin air.

Of course, YOUR money doesn't come out of thin air. You have to go to work while sick, drive in inclement weather, put up with all manner of psychopathic games with a boss's boss etc plus work your butt off to come up with what will easily amount to 1/3rd of all of your income for 30 years. And as the owner of that note, the Federal Reserve will then own a third of all your productive efforts for most of your adult life. And they get that in exchange for, literally, nothing. All they did is write numbers on a ledger somewhere.

In addition, they provide a great deal of the funding that the government needs to operate when it is in deficit. This puts our government in debt to the Fed as well.

The Federal Reserve (i.e. “the Fed”) is a coalition of privately owned banks that literally prints money out of thin air, issuing it as debt without also issuing the money needed to pay back that debt, and

thereby underpinning an economy that requires infinite (and ultimately unsustainable) expansion merely to stay afloat. As part of this process, the “finance” sector of our economy, though it creates nothing, concentrates nearly all the wealth in our society in the hands of a few who did nothing to create it.

This, in turn, leads to a situation where public officials can be bribed in a legal way to serve the interests of high finance, rather than the interests of the people they represent, or the Constitution they are sworn to uphold. By tweaking the interest rate one way or another, the Fed can influence whether or not an incumbent gets re-elected. That’s an awful lot of power being held by people whose names most of us don’t even know.

Because this fundamental corruption that lies at the heart of many of our problems has been allowed to fester for over 100 years, our children and children's children continue to be sold into declining standards of living and lower levels of security.

Inflation, corruption, growth with no purpose and consequent environmental damage, along with redistribution of wealth to a financial elite are just the tip of the iceberg of the harm worked by the Federal Reserve System.

Despite the fact that most people don’t notice, there has always been a sizable minority of people who have figured out the scheme, and been enraged by the Federal Reserve System which has served to make a handful of international bankers, along with globalists and their close friends insanely rich beyond all imagining, while ordinary people struggle to remain just two missed paychecks from bankruptcy. And while our elected officials say one thing to us in order to get our votes, when they assume office – whether Democrat or Republican – their legislation always serves the interests of that handful of largely anonymous and personally unaccountable monetary elites who literally print money into existence, and have never, in 100 years, been audited. Our entire economy is set up to funnel every spare dollar into the coffers of finance capitalists rather than those who work hard and innovate.

I will not dwell further on the Federal Reserve except to say that those who have recognized its evil have not been able to awaken their countrymen to the problem in order to have it addressed, and so have decided to take a variety of alternative routes, and among these has been the creation of alternative currencies.

And this is the origin of eGold and the Liberty Dollar.

Created as a protest against the Federal Reserve System, the Liberty Dollar was a minted silver coin whose value was set at a specific exchange rate for U.S. dollars. Because it was backed by a verifiable physical asset, it could not be inflated at random or used as a Ponzi scheme.

As the Liberty Dollar became more widely accepted and an increasing number of small businesses started accepting it, its creator also issued paper warehouse receipts for a specific amount of silver that was stored at The Sunshine Mint so that every piece of paper in circulation was backed by actual silver. This was more convenient than carrying around actual silver. As the last phase, the founder started a



digital version with secured warehouse receipts being transferred electronically, which would have allowed the Liberty Dollar to serve as payment for online transactions.

Although nothing about the Liberty Dollar resembled any currency of the United States, the creator of the Liberty Dollar was nevertheless jailed for "counterfeiting" and all of the silver and related assets were seized by the government.

Although eGold addressed the fundamental issues of the Federal Reserve, it also addressed another looming issue that has become even more urgent in recent years: privacy.

There is an increasingly emerging environment that even though it might be illegal to discriminate against you on the grounds of your race or sex, it is permitted for any corporation, including providers of basic banking services, to discriminate on the basis of political views. The fact that corporate entities are allowed to fire people, or deny them access to banking services on the basis of their politics is about the most un-American concept imaginable, but that is unlikely to change.

Likewise, there are a host of other monetary controls in place that the high and mighty fly above, but can become onerous for people trying to transact business in foreign countries or even send a few dollars to a distant friend in need.

Unlike the Liberty Dollar, eGold skipped the minting of coins and instead used encryption technology to make an electronic receipt for an amount of gold that was stored in an audited vault. But the primary focus of eGold was privacy and security. Your transactions were nobody's business and could be conducted completely outside the scrutiny of banks and regulations.

Based on the island of Nevis with strong financial privacy protections, eGold promised privacy, the ability to transact business anywhere in the world with minimal fees or barriers, and transactions that, unlike those done using bank cards, could never be reversed. At one point the ecosystem for eGold was big enough that people were reselling from the Amazon catalog, and you could register Internet domain names using eGold.

eGold was pretty much airtight except for one little detail: even though the U.S. government has no jurisdiction in Nevis, it has total jurisdiction over any person physically in its territory, and the founders of eGold resided in the United States.

So, the government found a way to arrest the founders of e-Gold and ultimately convicted them of "operating a money transmittal service without a license." This was even after they had requested a government investigation to see if they needed such a license, and the government told them they did not. But, once they "copped a plea" and were convicted, they were no longer eligible to obtain such a license and for all practical purposes eGold was shut down.

Both the Liberty Dollar and eGold were legitimately run enterprises backed by real and verified gold and silver stored in physical vaults.

These were great ideas, but they underestimated the evil that our government serves. When something poses a risk to the status quo, some sort of pretense will be dreamed up in order to justify shutting it

down. And if the physical backing assets or the people running it are within the physical jurisdiction of a compromised government ... well.

And this is where cryptocurrency enters the picture. The creator of Bitcoin left the following message in the very first block in the chain: "Yes, we will not find a solution to political problems in cryptography, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own. It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though."

Although the Liberty Dollar and eGold were based on physical assets as a way of preventing fraud of the sort that the Federal Reserve perpetrates, an alternative currency doesn't have to be backed by precious metal. And precious metal can't serve as a source of security when it can be arbitrarily seized at any time under the most flimsy of pretenses. Cryptocurrency uses advanced cryptography to avoid fraud, and in this way removes the vulnerability of centralized asset storage.

Cryptocurrency works on the basis of a public ledger of all transactions that have ever been made, and copies of that ledger are distributed among millions of computers (called nodes) all over the world. (Contrast this with a Federal Reserve that has never been audited.) As each new set of transactions is added to the ledger, those transactions are validated with a cryptographic hash in such a way that each new transaction depends on the previous one, with the transactions forming a chain (called a blockchain). Going back and changing one of the transactions would be practically impossible, and if anything went terribly awry there are millions of copies of the original ledgers to demonstrate that funny business was afoot.

The value of cryptocurrency lies primarily in the willingness of someone else to accept it in exchange for a good or service. But at this point with billions of dollars of cryptocurrency out there, and even Bitcoin ATMs that you can use, acceptance is a fait accompli. The second aspect is that because all of the processing that makes it work is spread out all over the world, and there is nothing centralized, nobody to arrest and no physical assets to seize, cryptocurrency has a level of resilience that eGold and the Liberty Dollar could never have.

First generation cryptocurrencies such as Bitcoin and Ethereum have public ledgers. If you publish your address so others can pay you, it is a simple matter for anyone who wishes to see how much of that cryptocurrency you own, who sent it to you, or who you sent it to. In fact, Coinbase, a U.S. based cryptocurrency exchange, will summarily shut down your account if it sees you sending cryptocurrency to support various people with whose politics it disagrees.

Monero solves that problem.

Monero is similar in concept to Bitcoin except that it has a few twists that work in people's favor. The first is that it is virtually untraceable, which means that unlike Bitcoin or bank transactions, nobody has a record of what you have purchased, or from whom. Nobody but you has a record of how much is in your Monero wallet.

The second major twist is that it is specifically configured to be “ASIC resistant.” In practice, this means that anyone with a computer anywhere in the world can mine Monero (more about mining later), which means that unlike Bitcoin, Litecoin and similar cryptocurrencies, it doesn't have its transactions dependent on countries or regions with cheap electricity. If you were to look at a global map of Bitcoin nodes, you'd find a very heavy concentration in China. But if you were to look at a similar map for Monero, you'd find most of the nodes in Europe and North America with quite a few all over Asia.

This makes Monero the most private, and the most resilient cryptocurrency. The bottom line is this: Monero is the mechanism that will allow us to have a parallel private economy. It's as simple as that.

And that parallel private economy means security, liberty and the ability to do the things we would otherwise never be able to do.

## Word to the Wise on Speculation

Everything I'm saying here applies to all cryptocurrencies, including Monero. I am using the example of Bitcoin because that's what is most familiar and where the hype has been.

There are a lot of people who bought Bitcoin or other cryptocurrencies back when nobody had heard of them, and they cost less than 1/1000th of what they do today. As a result, they became millionaires when Bitcoin values appreciated in late 2019. That was a great call on their part, and I'm pleased that it worked out.

As is so often the case, other people look at that situation and they want to hop on the easy money train, but they are trying to accomplish the same thing by buying Bitcoin at a price of \$8,000 rather than \$2. For reasons that should be pretty obvious, the amount of appreciation potential when it costs \$8,000 is a lot less than it would have been for those who bought it at \$2.

Although it is not completely analogous, this is what so often happens with stocks. The big guys have early information, buy at a lower price, and by the time the information filters down to the average investor, most of the appreciation has already happened. The big guys made 500% on their investments, while the average investors are lucky not to lose value.

This is how hype trains work, and why those who jump on them tend to lose. The hype occurs after the largest gains have already occurred.

But let's go back to first principles: cryptocurrencies were invented, not as investments, but as a way to enable commerce that would otherwise be prohibitively expensive or impossible because standard credit card processors like Stripe selectively "black hole" people who don't share their politics. Bitcoin and similar currencies give us a way around that – and, in fact, a way to bypass the banking system altogether, which can allow us to keep our identities more secure. It is a manifestation of the true spirit of the Fourth Amendment.

In addition, cryptocurrencies (usually) have transaction costs of less than a penny, which is a lot less than the transaction costs charged by the credit card processing companies. This can be especially beneficial to businesses that do a high volume of low-cost sales, where a standard cut of as much as \$2 taken by the processors for each sale can cut heavily into profits.

These make cryptocurrency a great way to transfer value and facilitate a parallel economy.

But as investments, cryptocurrencies are very speculative and you are as likely to lose value as to gain it. Let me provide a thumbnail sketch of how this works via an example.

Pretend you sign up with BigXchange, the largest exchange for Bitcoin in the United States, and you purchase \$1,000 worth of Bitcoin. Pretend 10,000 of your closest friends do the same. Now, BigXchange has a cool \$10,000,000 in its coffers, but it actually has to use that to pay the people from whom it obtained the Bitcoin that it sold you. We will pretend, generously, that BigXchange employees

work for free and that the enterprise has zero overhead and works by magic. So BigXchange only gets to keep a portion of the fees it charged for the exchanges. If they make money – and they do – it is from transaction fees alone.

Pretend, further, that the value of Bitcoin climbs so that your original \$1,000 investment is worth \$5,000.

Okay, let's digress a moment. What does that mean? Where does that value come from?

Just like a stock, that value comes from transactions that are taking place on Bitcoin exchanges that are very similar to stock exchanges, and they reflect what people, in real time, are willing to trade for Bitcoins. But this reflects only a small number of people and a small number of Bitcoins compared to those that are being held in wallets.

As I write this, there are currently fewer than 18,000,000 Bitcoins in existence and, due to its design, there will never be more than 21,000,000. The peak trading volume of bitcoins was about \$5B at a time when the Bitcoin was trading at \$15k so the total market capitalization was \$255B. So all of that trading really involved only about 330,000 Bitcoins changing hands – or about 2% of existing Bitcoins. And most of that movement was from one wallet to another for purchasing goods and services, rather than outright purchases of Bitcoins at that price.

So the valuation of Bitcoins at \$5,000 or any particular price is NOT a reflection that all Bitcoins could be exchanged for that much national currency. Instead, it reflects the fact that some people, somewhere, were willing – at a given moment – to purchase a tiny percentage of existing Bitcoins at that price. And that is an important thing to consider.

Now, let's go back to our imaginary scenario. You and 10,000 of your closest friends, who purchased \$1,000 worth of Bitcoin from BigXchange, are now all holding \$5,000 worth of Bitcoin. This is a godsend because you could really use the money, so you all rush over to BigXchange and trade in your Bitcoins for national currency (dollars) to be deposited to your bank accounts.

And that's where things start to go wrong.

Rudimentary economic understanding tells us that there are far fewer people out there inclined to spend \$5,000 to buy your Bitcoin than there are who will spend \$1,000, simply on the basis of far fewer people having that sort of money available to spend.

What happens if the exchange can't find 10,000 people who are willing to pay that higher price?

And this is the key I am getting at. In our scenario, the exchange only has the fees in its pocket, plus whatever it is able to RE-SELL your coins for.

This whole deal works fine only when a tiny proportion of total Bitcoin is exchanged for currency, and that is matched by a similar amount of currency being exchanged for Bitcoin. If that gets out of whack – by, for example, more people wanting to sell than are willing to buy, here is what happens:

When 10,000 people show up to liquidate their Bitcoin, the first few – maybe 500 of them – will get the full “market price.” But as more and more show up to liquidate, the price drops ... and drops ... and drops. That is because BigXchange, even if run by the most perfect and most ethical people on earth, is not the Federal Reserve. It cannot create money out of thin air – *it is completely at the mercy of willing buyers and willing sellers*. And this is one reason why you see the value of cryptocurrencies fluctuate so much.

The published value of a cryptocurrency reflects only a tiny proportion of it changing hands at any given time, and reflects only what a handful of people are willing to pay for it. It absolutely does NOT reflect what the value would be if the holders of a substantial portion of Bitcoin – say, 20% of it – decided to sell. If that were to happen, it’s value would drop like a rock. Even now with 5% or less being traded, its valuation is fluctuating wildly.

Also, consider that the intrinsic value of a cryptocurrency is zero. It is just bits in computers. This doesn’t mean they can’t have utility as currencies, but it means that as investments they are iffy at best.

National currencies fundamentally derive their value from the fact that their issuing authorities require you to use those currencies to pay taxes. If you don’t pay your taxes as prescribed, using their currencies, ultimately a large number of heavily-armed people without any sense of humor will show up and take you into custody. So national fiat currencies rely on the fact that the most productive people in a society want to avoid trouble with the government, and this is a rather reliable means of maintaining their value.

Previous alternative currencies that the federal government shut down with extreme prejudice were backed by physical assets: eGold and the Liberty Dollar were backed by gold and silver kept in safes. In a rational world, these currencies were indeed a secure store of value. But as such, they presented a substantive risk to the status quo, and hence they were shut down with their central purveyors taken into federal custody.

Cryptocurrencies, just as they have nothing backing them as an investment, have nothing backing them as a currency except for people’s willingness to accept them.

So what’s my point?

Two things.

First, cryptocurrency is exceptionally volatile in terms of its pricing, and investing in it is pure speculation. You may win, you may lose. Use your own judgment, but it’s not something I’d personally recommend. If you can’t afford to lose the money, don’t put it in a cryptocurrency.

Due to its decentralized nature, cryptocurrency in general has a lot of positive potential to help us build a parallel economy. So I’ll write more about this in future chapters. But try not to get caught up in the hype of using cryptocurrency as an investment vehicle. Your odds of being a winner aren’t great.

# Safeguarding Your Privacy

The financial sector and large corporations, collectively referenced as "woke capital" have declared outright war on anyone who doesn't conform to thoughts they deem acceptable.

As I mentioned in the introduction, the fact that they might currently be exercising that prerogative against people you find reprehensible doesn't make you immune. The Internet, they say, is forever. That is, today you can express an opinion on social media that is 100% approved by the powers-that-be, but twenty years from now when the limits of acceptability have changed yet again, you may find yourself – or your kids – denied opportunity because of that.

You see, people are asking the wrong question. The question they typically ask is "Should so-and-so, whom I believe to be evil because he or she thinks bad thoughts, be banned from accepting credit cards for her perfectly legal enterprise?" The correct question is: "should banks and other corporations be allowed to discriminate against people based on their political opinions?"

The answer to that question, in my opinion, is no. But nobody has promoted me to dictator, so we have to contend with a world in which your basic freedom to obtain the necessities of life such as food, shelter and water can be denied to you on the basis of an opinion you expressed a decade prior, and perhaps you didn't even really mean.

The reason our Founding Fathers insisted on a secret ballot was so people would not fear retaliation for exercising their political opinions. And with regards to speech, noting the precedent of our founding fathers who wrote using pseudonyms, the Supreme Court has ruled that anonymity is necessary in order for free speech to be adequately protected. But campaign finance laws require public disclosure of both your name and employer if you contributed even \$10 to a political campaign.

So naturally there has been an effort at data mining that has been used whereby people who have made small donations of \$10 or \$20 to initiative petitions, or even signed them to allow them access to the ballot, have been "exposed" for this, and activists have gone through those lists, calling employers and attempting – sometimes successfully – to raise a ruckus and get people fired from their jobs. This is a case where disclosure laws ostensibly created to keep politicians from selling out have had almost zero impact in terms of their intended purpose, and are instead misused to stifle freedom.

The fact that these sorts of things are happening now on a pretty large scale, even if it isn't making the news for some reason, should make us all worried. How long will it be before someone who signed a normal petition gets fired because of some activist, and as a result their spouse dies from cancer because they have no insurance? When does it escalate from indirect murder to direct murder, or homicide in self-defense? I don't know, but it is best to avoid the whole situation if we can.

All of the foregoing should underscore the importance of being able to keep your finances at least somewhat private, and that you should also have an alternative means of doing transactions that can bypass chokepoints. And that alternative is cryptocurrency.

To start a cryptocurrency wallet, you don't need anyone's permission and you don't need to provide any ID. There are numerous applications for allowing you to keep cryptocurrency wallets of various sorts on a variety of devices. Although there are practical considerations, there is no limit to the number of wallets you can possess. To receive crypto, give your recipient address to the sender. To send crypto, you send to the wallet address desired.

Where identification enters the equation is via exchanges. Typical exchanges will require photo identification, linkage to a verified bank account and so forth so that they know precisely who you are. This only impacts your privacy for the wallet accounts created on that service, though. So such wallets ought not be used directly. Since the wallet addresses of numerous people are widely known, exchanges will often disable your account if you send or receive funds from accounts who have politics of which they disapprove. So instead, send from your exchange wallets to a second wallet, and use the second one for sending or receiving funds.

This works fine for donations to dissident podcasters and such. But especially when using bitcoin, ether, litecoin and their variants, you can still be tracked with a dedicated effort. To break that chain, you have to convert to a privacy-oriented cryptocurrency such as Monero (XMR) via a currency converter such as changelly.com. So, you buy Ether or Litecoin on a regular exchange, use Changelly to convert it to XMR in your separate XMR wallet, and then pay via that wallet. This way, your privacy is preserved.

Using XMR, you can keep transactions completely secret, even in regard to who paid whom, and thereby retain your privacy. Furthermore, you can accept XMR as a form of payment on your website, and nobody will be able to cut off your ability to get paid. Later, if you need dollars, you can use a currency converter to put that currency into a standard exchange and then liquidate it.

There are quite a few companies who sell perfectly legal items that have had a lot of trouble with credit card processors, and have switched exclusively to cryptocurrencies of various sorts. The startup cost for using cryptocurrency is negligible compared to maintaining merchant accounts. And although I explained the risk of high fees in the preceding chapter, for the most part transaction fees for cryptocurrency are far lower than for credit and debit cards; there is no such thing as a chargeback, and your funds are available within minutes.

So cryptocurrency in general gives better privacy than a credit card and can allow you to do business online when card processors have denied you that ability. Using an independent wallet that you fund from your exchange wallet gives even greater privacy, and converting those funds to Monero gives the greatest privacy of all. You can start accepting payments via the Internet with negligible startup costs and nobody can shut down your account.

A word of warning: cryptocurrencies are unstable, so don't use these cryptocurrency wallets as savings accounts unless you can afford to lose their value. Furthermore, take all precautions not to lose the passwords or creation keys because if you do, there is no getting them back.



Keep in mind that just as people sometimes use U.S. Dollars to facilitate evil things, they can also use cryptocurrency – so be careful to give evil people a wide berth.

Instead, use cryptocurrencies as an avenue to enhance your privacy and autonomy.

# How Cryptocurrency Works

I have talked with dozens of people who are profoundly confused about cryptocurrency. The purpose of this chapter is to make sure anyone who reads it has a solid understanding of how cryptocurrencies work in general. This is presented from a high level view so it is clear how all the moving parts work together. In subsequent chapters, I'll delve into the details of how each part works and how to use them.

At the very beginning are two things: a wallet, and a ledger. Let's start with the wallet.

The term "wallet" is used for a very specific reason: it is like a physical wallet to the extent that if you accidentally drop it into the Mariana Trench in the Atlantic Ocean, it's gone forever. If you hand it over to someone else or give someone else access to it, they can do whatever they please and there is absolutely nothing you can do to change what they have done.

A wallet is absolutely NOT analogous to a bank account, because if you've ever had fraudulent charges, you just call the bank (often they call you first!) and have them reversed. If you forget your password to log in, you call them and give them your identifying details, and they will reset it for you. None of these is applicable to a cryptocurrency wallet.

A cryptocurrency wallet is fundamentally composed of three things: a public cryptographic address that anyone can use to send you currency, a private cryptographic key that allows you to have access to that currency and to spend it, and a password for securing the private key. That is all that a wallet contains. The virtual coins themselves exist solely on the blockchain, but it is your private key and password that demonstrate your ownership and control of those coins. If you lose either your private key or password, those coins will forever sit there inaccessible to anyone.

In practice, people speak of wallet software. Wallet software serves as a convenient place to keep your keys and access the blockchain for purposes of sending and receiving funds. It scans the chain to tell you how much cryptocurrency you have. Wallet software has many bells and whistles, but at its most basic level it is just a convenient place to hold your real wallet, which consists of your password-encrypted private key.

The ledger – which contains all transactions from all wallets – is called the blockchain, and I'll explain why in a minute. This shared ledger is maintained in duplicated form across millions of nodes. Each transaction is combined with a number of other transactions, and added to a block on the ledger. Ascertaining that your particular private key has access to a certain amount of cryptocurrency is accomplished by scanning the transactions in that shared ledger for those pertaining to your wallet, and adding and subtracting the transactions that it finds.

So if you start off with zero, buy one coin and then send 1/4 of a coin to someone else, the shared ledger records these transactions and your wallet will scan the ledger for transactions pertaining to its address, and report that you have access to 3/4 of a coin. Simple.

But what would keep someone from going into that shared ledger and changing a few numbers around?

This is the purpose of the blockchain. The transactions in the ledger are kept in blocks. As each new block is added, it is combined with the block just prior, and millions of miners (more on those shortly) compete to find a cryptographic hash of the combined blocks that meets a certain criteria. This is a tough criteria, so it will take millions of miners computing billions of hashes to find a suitable solution. Once a solution is found and another few miners also find it, the transactions in a block are finalized along with its hash in the ledger – a ledger composed of blocks chained together, each dependent on the previous block.

The ledger is effectively immutable. If you combine the fact that the ledger is duplicated among millions of nodes with the difficulty of going back even a couple of blocks and recomputing with altered values, the blockchain itself is practically impossible to hack. (Exchanges can be hacked, computers can be hacked. Even your wallet can be hacked if you are not careful. But the blockchain itself seems to be effectively unhackable.) And this also explains why a transaction can't simply be reversed. An honest merchant can refund your money in a new transaction, but the original transaction is itself irrevocable, just like paying with cash at a yard sale.

A node is a computer that keeps a copy of the entire blockchain, adding blocks to that copy as they are secured. Some nodes only keep a copy of the blockchain, but many wallets allow your computer to also become a node. The existence of numerous duplicated copies of the blockchain serves to make it impossible to alter.

Because the blockchain is public, there are companies that exist whose sole purpose is to track every transaction on the ledger in order to use the information for taxation purposes or to gain other information. So don't assume most cryptocurrency is untraceable, because a lot of it can be traced. And it is written in stone. Exchanges likewise report any "gains" in your accounts to taxing authorities. (So please make sure you report and pay all applicable taxes. Taxing authorities are notoriously relentless in pursuit of people they think are cheating the system.)

But what about these so-called miners? What motivates them to spend gobs of money on electricity or the extra cycles on their computers just to validate and lock in your transactions?

The answer is that every transaction in cryptocurrency is processed with a fee. And the miner who successfully validates that transaction gets to keep that fee.

In practice, unless someone owns an entire personal data center, their odds of validating a transaction and keeping the fee are pretty low. So what most miners do is join a collaborative called a mining pool. When any member of the pool successfully validates a transaction, that fee goes to the pool and is distributed among all the members in proportion to how much computing power they contributed toward the effort.

In addition, there is a sort of "Easter Egg" built into the algorithms such that every once in a while a new coin is "minted." The miner who hits this very rare Easter Egg gets the entire coin, which may be worth thousands of dollars.

Because mining is computationally extreme, it runs the associated computers full blast and they gobble electricity like crazy. This is why a lot of mining is done in places with cheap electric rates, such as near Niagara Falls. If the electric rate is too high, it costs more than the payout from mining. So you don't see much mining in Hawaii. Solar power is a great option.

So, other than the rare Easter Eggs, how do you actually get cryptocurrency? Although there are a lot of ways I will discuss later, the most basic way is through an exchange. An exchange is like a consignment shop. If someone wants to sell coins at a certain price and you are willing to buy them at that price, the exchange acts as a go-between and facilitates the transaction, transferring the ownership of those coins from the original holder to you via a transaction on the blockchain. They do this for a fee, part of which goes to fund the miners, and the rest of which they keep in order to keep their lights on.

There are various types of exchanges, some of which deal with national currencies and some which don't. Those which will sell you crypto with a credit or debit card over the Internet universally adopt the same "know your customer" rules that banks use. Later, I will explain how to "break the chain" so that you can use these exchanges and still protect your privacy.

So there are five basic parts to the system: exchanges where you buy and sell cryptocurrency, a wallet where you keep that currency, a blockchain, nodes that hold copies of the blockchain, and miners who secure the transactions on the blockchain. That's the entire system in a nutshell.

## What Makes Monero Better

Now it's time to move from generalities into specifics, because this book is not about Bitcoin or Ethereum or other cryptocurrencies. It is about Monero because so far Monero is the only currency that has solved the problems alternative currency was intended to solve.

In general form, and without getting into math or other geekery, Monero works broadly the same as other forms of cryptocurrency described in the last chapter. It has wallets, nodes, a blockchain, miners, and can be acquired through exchanges (although these are limited, as will be described later).

But every piece of this works a bit differently for Monero than it does for the others, and that's what makes it special. Let's start with the wallet.

Again, a wallet is merely a private key secured with a password. The algorithms used for the Monero wallet will allow you to generate as many unique receiving addresses as you'd like, meaning you can literally have an address used for only one transaction. This is important, because if an address is used for numerous transactions it creates a profile, similar to the one used to generate ads on Facebook. With Monero this is less of a risk than with other cryptocurrencies, but it is still good to have this option.

In addition, the official Monero GUI wallet (available at [getmonero.org](http://getmonero.org)) provides (under the advanced tab) a set of words that you can write down on a piece of paper, put in a safe place, and use to regenerate your keys and recover your account in the event of a computer crash. The official wallet also allows you to run a full node, thus helping to secure the integrity of the blockchain, and also allows for using your Monero keys to sign brief messages so that their authenticity can be verified. It also has a lot of other more advanced functionality that is beyond the scope of this book. For our purposes, it lets you send and receive funds, plus run a full node. It also allows you to generate one-time-only receiving addresses, as well as organizing your funds into subaccounts.

There are other wallets available for Monero that are typically faster because they don't run a full node, but few that are more comprehensive. You will have to upgrade your wallet software every six months or so. (More on that later.)

Where Monero really stands apart, however, is with their version of the blockchain, and the algorithms they use. Their algorithms mix transactions together and obfuscate their sources, destinations and amounts as they are put into the ledger in such a way that they can only be unscrambled to ascertain balances by those with the keys to those balances. As a result, Interpol has recently stated Monero to be "untraceable." This applies even if you use the same address for multiple receipts. This solves the problem of privacy that eGold was initially intended to solve, and it has predictably annoyed nosy regulators calling for its ban. Thankfully, because of the way Monero is mined to secure its transactions, it's impossible to regulate.

The transactions in other blockchains are primarily secured through mining using ASICs (application specific integrated circuits that mine very quickly) that are quite expensive, and gobble electricity like there's no tomorrow. As a result, most of the mining is done in China where the ASICs are made, and the electricity is cheap. This means that if China were to crack down on such activity (and they have hinted that they may) the blockchains for a number of popular cryptocurrencies would be slowed to such a crawl that transactions would take days rather than minutes, and transaction fees would make it unusable.

Monero however is specifically designed using algorithms that can't be used on these ASICs, but instead works on a standard PC CPU. This means pretty much anyone can dedicate a small amount of their CPU to mining Monero while they are working, and will never notice it. And in aggregate these millions of decentralized PCs can make Monero work just fine while making it very hard to shut down.

In order to stay ahead of ASIC design and preserve its distributed nature, the algorithms used for Monero are updated about every six months, necessitating replacement of wallet and mining software.

When you combine the attributes described above, it becomes clear that Monero is something special in the world of cryptocurrency because it solves the problems cryptocurrency was invented to address. It's ecosystem is robust and its algorithms force it to be widely distributed so it is nearly impossible to censor. It has several layers of privacy protection that make it effectively untraceable. This makes Monero a perfect fit for bypassing the tyranny that credit card processors and banks like to impose, which can effectively shut wrong-thinkers out of the monetary system altogether.

# Installing Your Monero Wallet

In the previous chapters I've explained that a cryptocurrency wallet is composed solely of password-protected encryption keys that identify their owner as having sole claim to a certain amount of cryptocurrency, and that amount is determined by looking through an immutable ledger described as a blockchain. And wallets are managed with wallet software.

There are some other alternatives, such as online wallets and hardware wallets. But for now I want to keep this straightforward and safe, and describe using the official Monero GUI to set up your wallet.

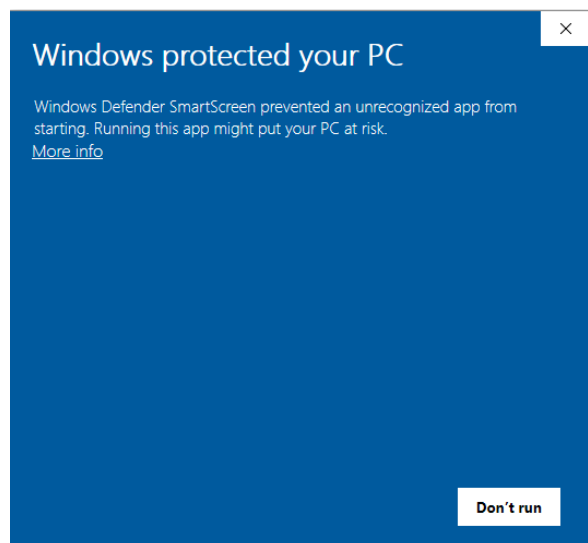
Before I get to the details, please consider that if your computer has been compromised, and your secret key is on that computer and a keylogger has been installed, hackers can take all of your crypto and there isn't anything that can be done about it. This is like cash, and unless you are made of cash yourself, you need to exercise due caution.

There are some basic things you can and should do for security. The first is keeping your antivirus and anti-malware software up to date, and despite its inconvenience, make sure it has run and kept everything clean before you get started. The second is to store your keys on a USB key rather than the computer itself (and to make a copy of that key). And the third is to write down – physically with a pen on paper – the mnemonic version of your secret key. I'm going to walk you through all of this, and provide illustrations when needed for clarity.

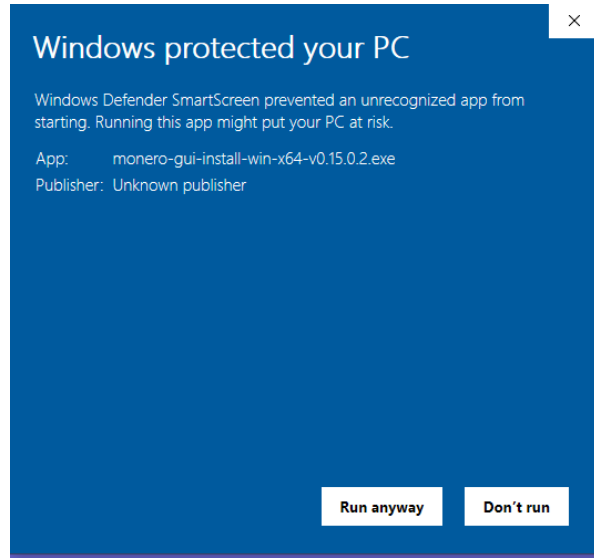
Go to [www.getmonero.org](http://www.getmonero.org) and download the latest version of the GUI Wallet for your operating system. If you want to verify its authenticity, follow the instructions for doing so on the website. Once you are satisfied with the authenticity of the program, go ahead and run it. This will install the latest Monero wallet on your computer. There are wallets available for Windows, Mac and Linux. I am illustrating the Windows version here, because it's a bigger pain to install.

## Installing the Software

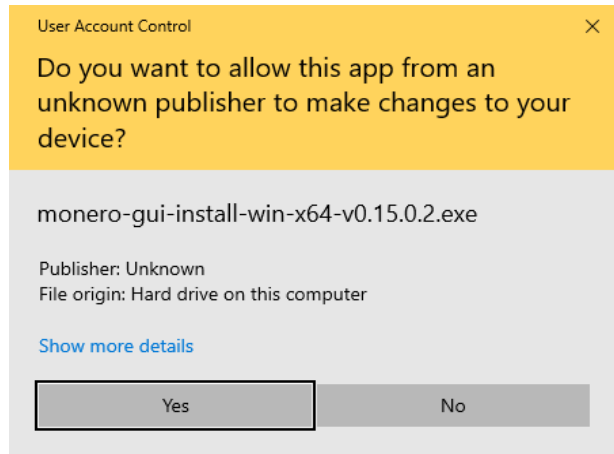
When you first try to run the installer on Windows, you get a dire warning. It's not obvious, but in order to run the installer, you'll first have to click the "More info" link.



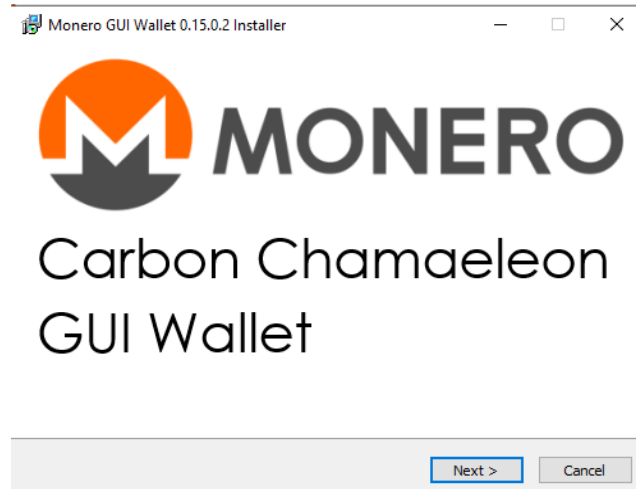
Then choose “Run anyway.”



And then select “Yes” to allow the app to install.

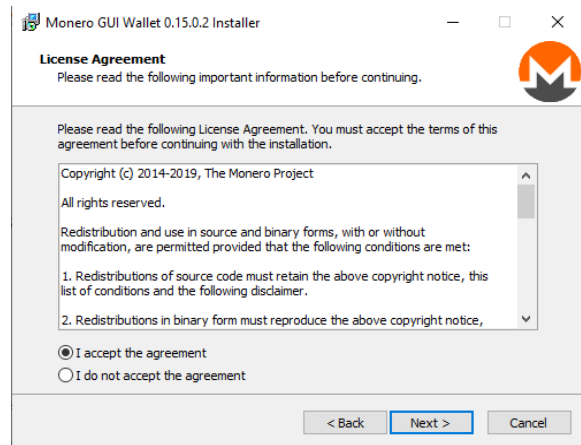


Finally the installer runs, so just click “Next.”

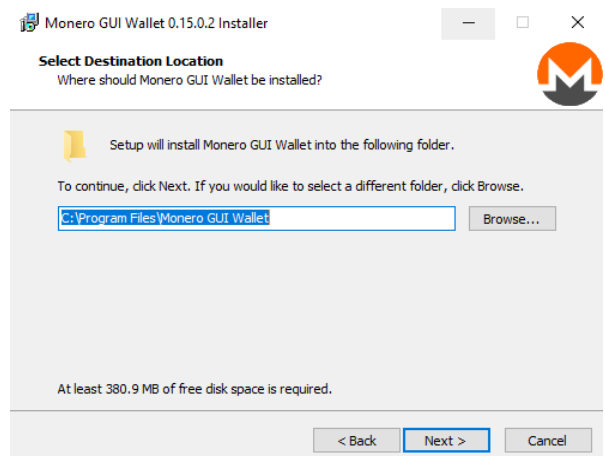




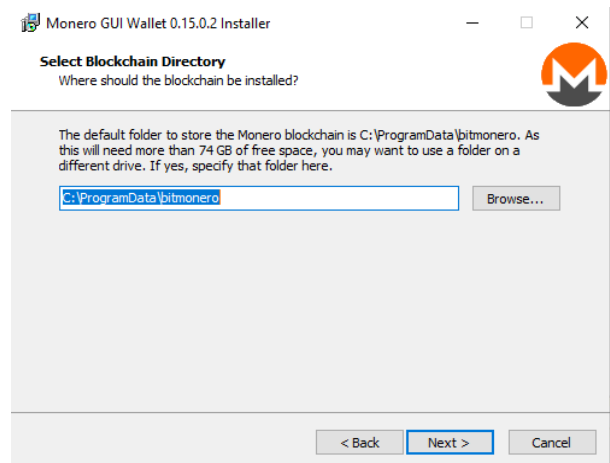
Read and accept the license agreement to continue.



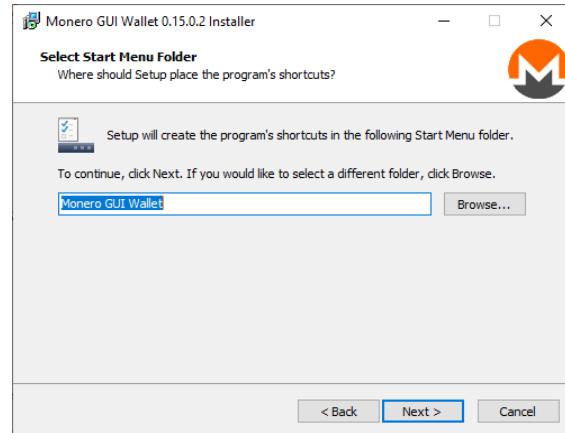
Select the location where you want your wallet software (not your keys) to be installed. It should work fine if you accept the default value.



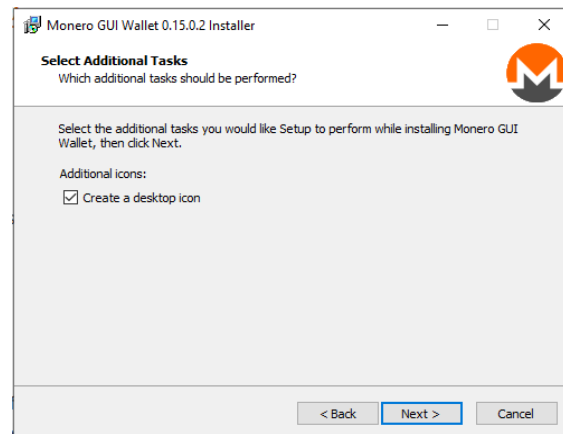
You need to pay attention to this one. If you are keeping your own copy of the blockchain, it currently takes almost 75GB of space. So select a drive with more than 150GB of available space, as the blockchain will grow by at least that much. (You might even use a separate disk for this purpose if you have a tower PC or the like.)



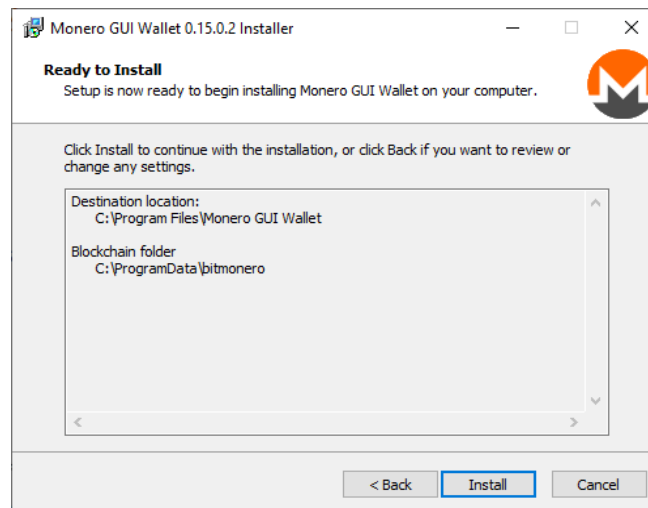
You can safely accept the defaults for this one:



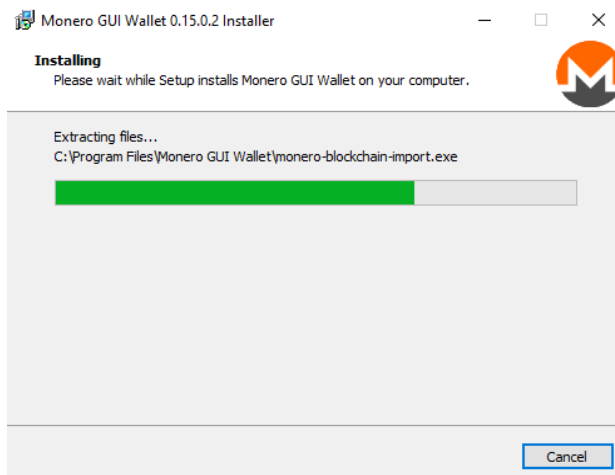
And this one as well:



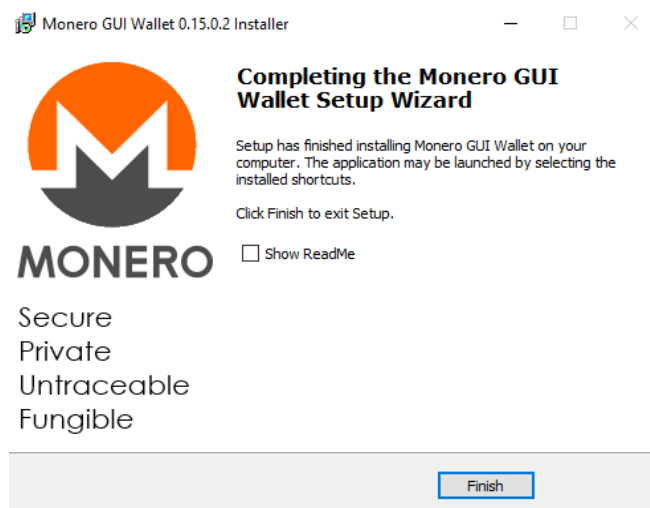
Now hit "Install" to give it the final go-ahead:



Relax for a couple of minutes while the installation completes.



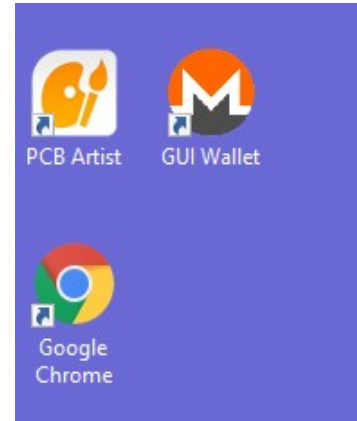
Click “Finish” to complete the installation.



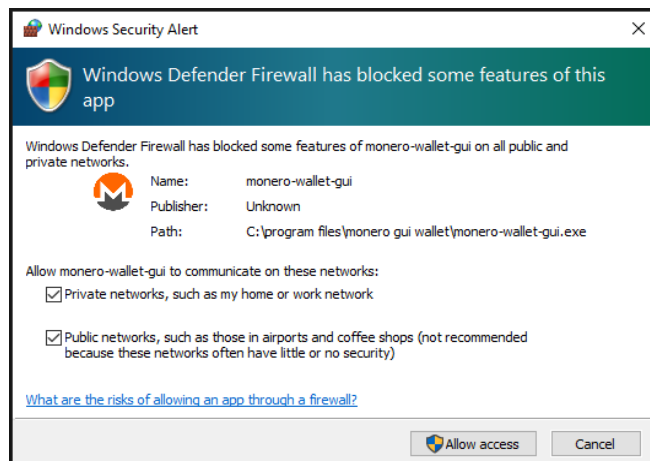
## Setting up Your Wallet

Now that you have the software, you need to set up your wallet so that you can send and receive Monero!

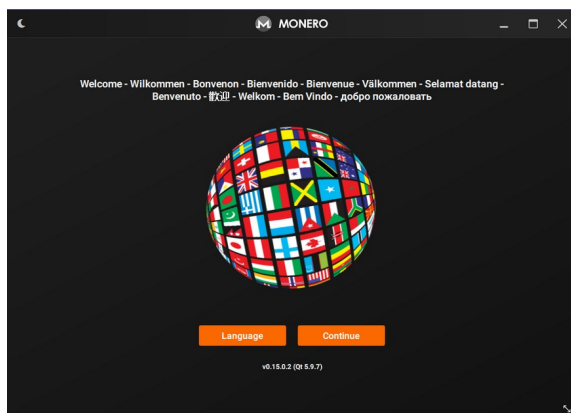
You can start by clicking the desktop icon that the installer put on your desktop:



Because the Monero wallet software connects to the blockchain and to other nodes, you need to give it permission to connect to both private and public networks when you run it for the first time.



The first time you run the Monero wallet software, you get an opportunity to choose your language if the one it is using (which it determines by asking your operating system) is incorrect. If you are satisfied with the language, click on “Continue.”



This selects the “mode” in which your wallet operates. All three modes have benefits and drawbacks.

“Simple Mode” will get you up and running most quickly, because it doesn’t have to download the entire blockchain to your device. It can take a while to locate a node, and every once in a while it will find a node with an outdated version of the software, and give you a “node version mismatch.” Be patient and it will eventually find a properly matching node.

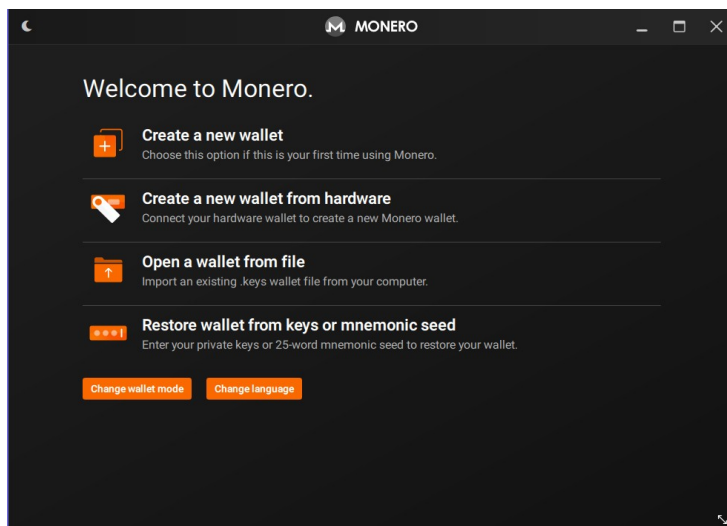
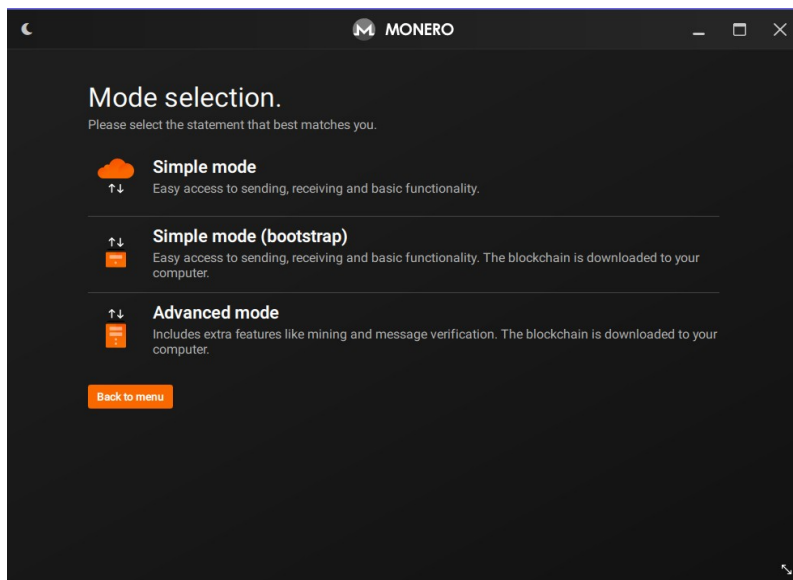
The “Simple Mode (bootstrap)” downloads the blockchain to your device, and this process can literally take hours the first time it happens, during which you can do nothing with your wallet. Thereafter, each time you open your wallet, it will download whatever transactions took place while you were away, which usually takes only a few minutes. This gives you the greatest privacy while still giving you a simple interface.

“Advanced Mode” is for the guru you will eventually become, and allows for signing messages cryptographically and other advanced functions not covered here.

For our purposes, I suggest that you select “Simple Mode (bootstrap).” I am using “Simple Mode” for my demonstration account that will only transfer a tiny amount of Monero, so there’s no risk. But for your greatest security, as stated, you should use “Simple Mode (bootstrap).”

Before this step, put a USB key in your computer, and create a folder on the key called “Monero.”

Now, on this screen, select the option to “Create a new wallet.”

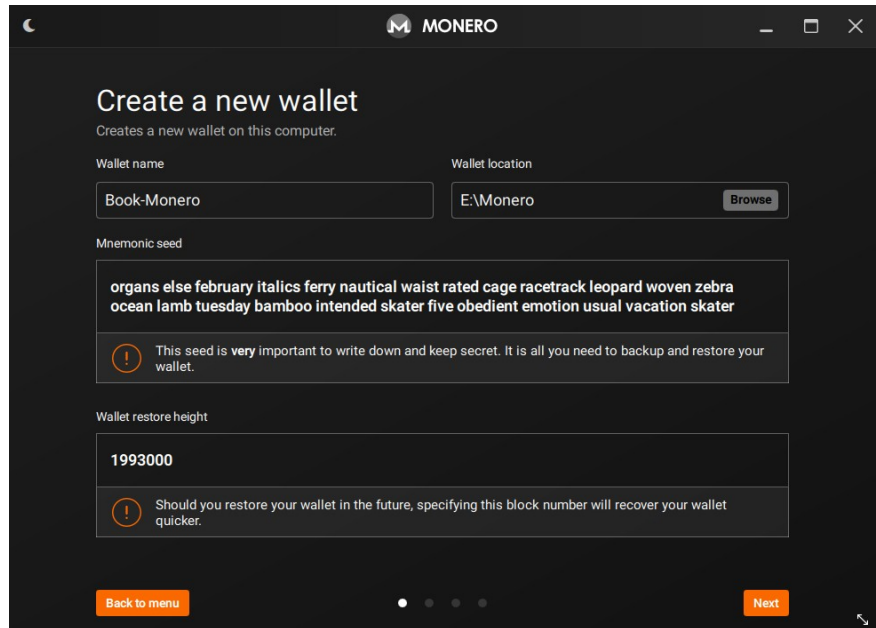


Here is where you get out a piece of paper and a pen!

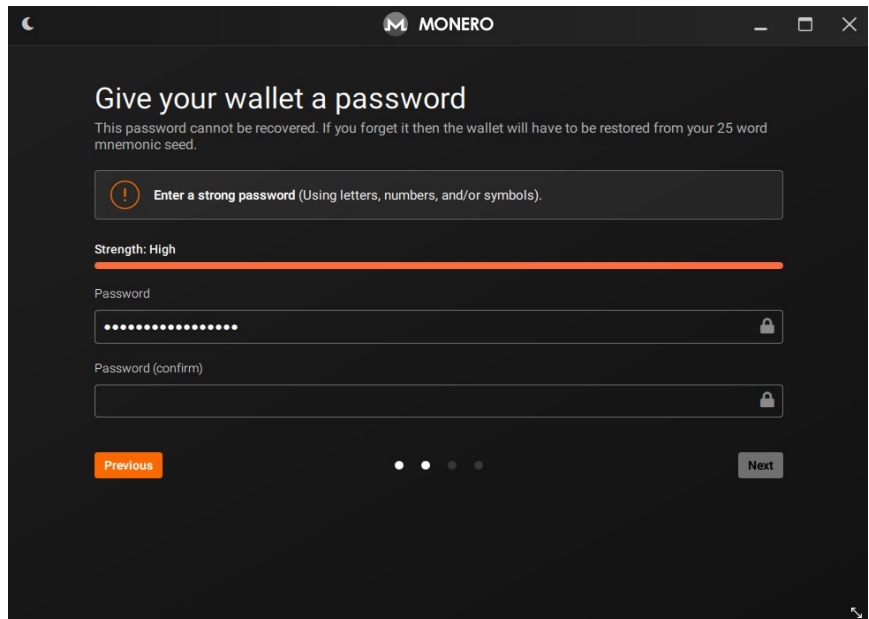
Set the wallet name to whatever you'd like. It is only used internally by the program and nobody else ever sees it. But just in case, it's probably wise not to use profanity, a password, etc.

Use the Browse button to select the Monero folder you created on your USB stick.

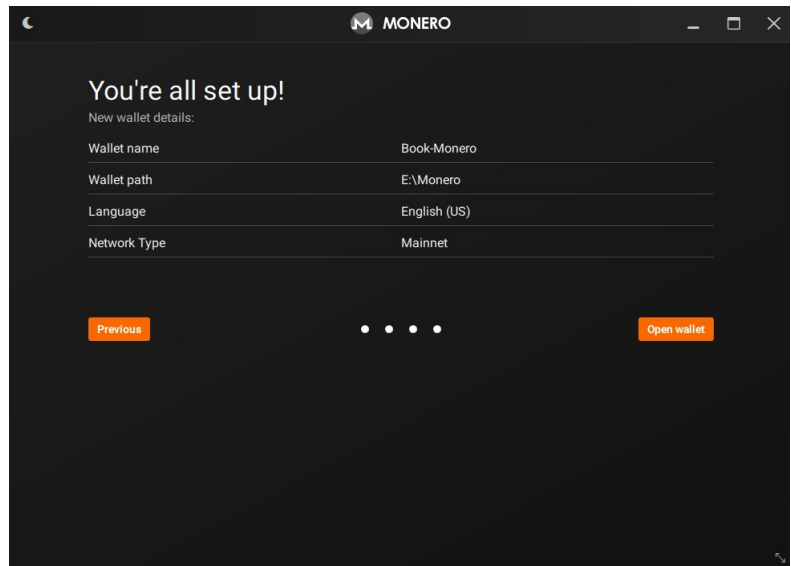
Then, use your pen and paper to write down, exactly and perfectly, the words in the Mnemonic seed, as well as the "Wallet restore height." Put these in a safe place because in the event your USB key is lost or damaged, you can use them to restore your wallet.



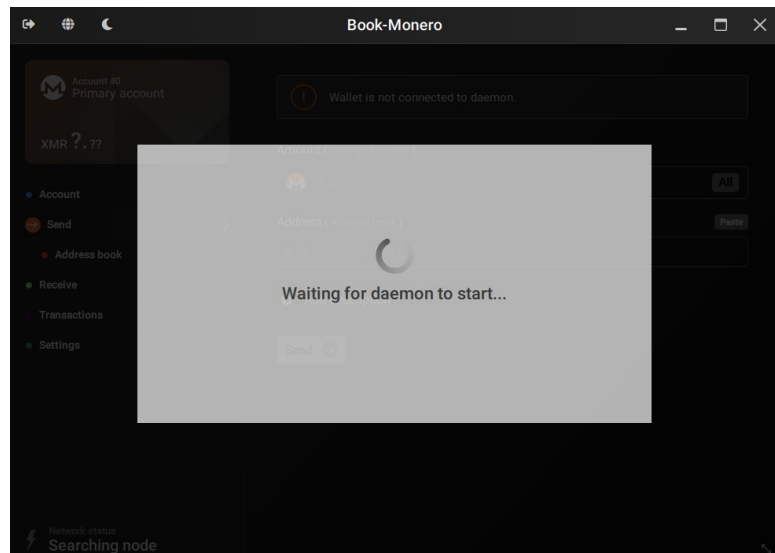
Here is where you select a strong password. If someone has your USB key, or physical possession of anything else where you have stored your wallet, if they can guess your password by using the name of your spouse, child or favorite football team, then they can steal all of your Monero. So select a strong password. If you are afraid you will forget it, write it down on a piece of paper and put it in a place separate from where you wrote down the mnemonic seed. When you are done, click Next.



Now just click “Open Wallet” to get started!



When your wallet first starts, it will start a process that runs in the background (called a “daemon”) that keeps track of the blockchain. After that is done running and everything is synchronized, you are good to go!



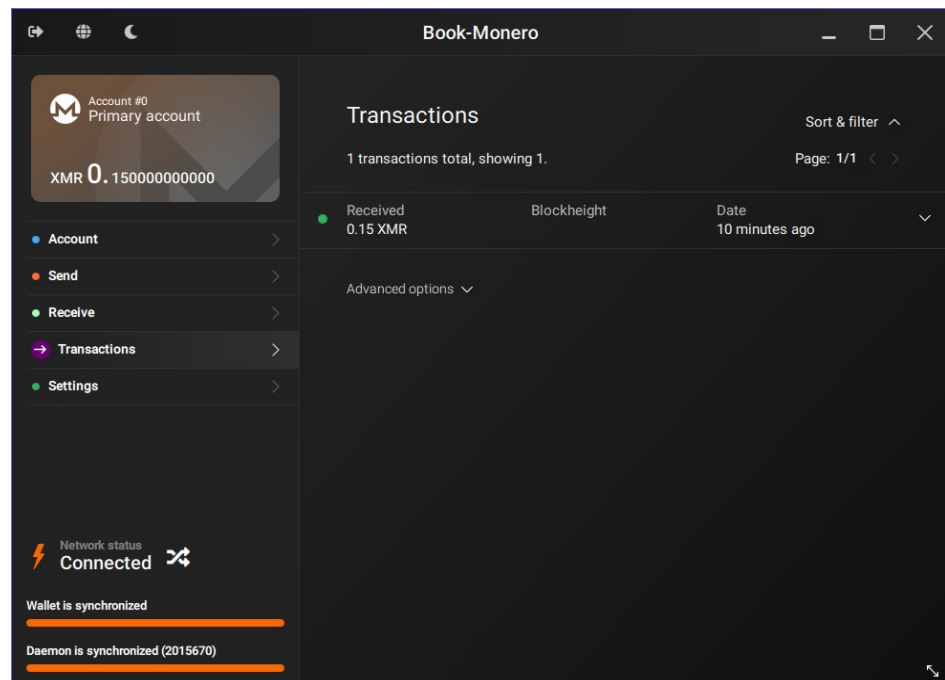
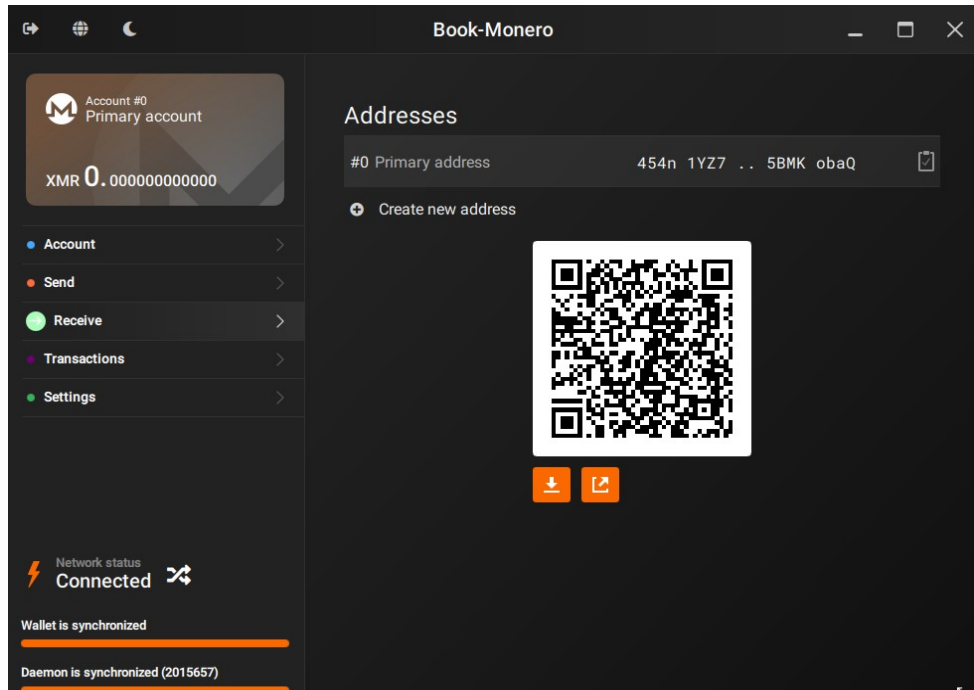
# How to Send and Receive Monero

This chapter covers how to send and receive Monero using your wallet, both of which are surprisingly easy. All you need in order to send, is the Monero address of the recipient. In order to receive, just give your Monero address to the sender.

## Receiving Monero

You can find your reception address by clicking Receive in the wallet interface. You'll notice a field called "Primary address." To the right of that is an icon that looks like a clipboard with a check mark inside. If you click that, it will copy your address to the clipboard, so you can paste it anywhere you'd like, such as an address on a web page seeking payments or donations, or send it to your friend who needs to pay you for a bike tire.

Once someone sends a payment, it will take about 20 minutes to become spendable. You can check the status by clicking on the Transactions link in the menu on the left. There, you can see a transaction in progress for about 0.15 XMR. (About \$9 - \$10 at

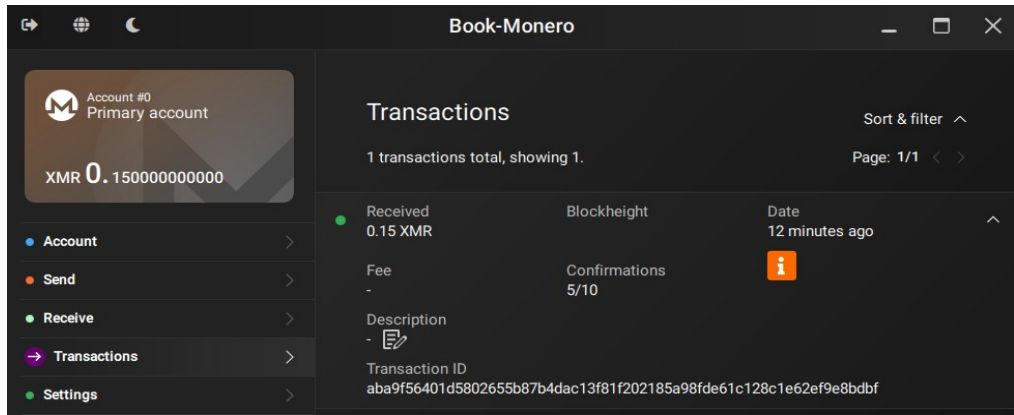




the time of writing.) If you click on the downward pointing arrow, you can see the status of the transaction confirmations.

(Continued on next page)

Here you can see the transaction in progress. Notice the “Confirmation” section where it says 5/10. A transaction is not made a permanent part of the blockchain until ten miners find the exact same cryptographic hash, which takes about 20 minutes.



Eventually, the transaction is confirmed and completely irreversible. And now this account is the proud owner of 0.15 XMR!

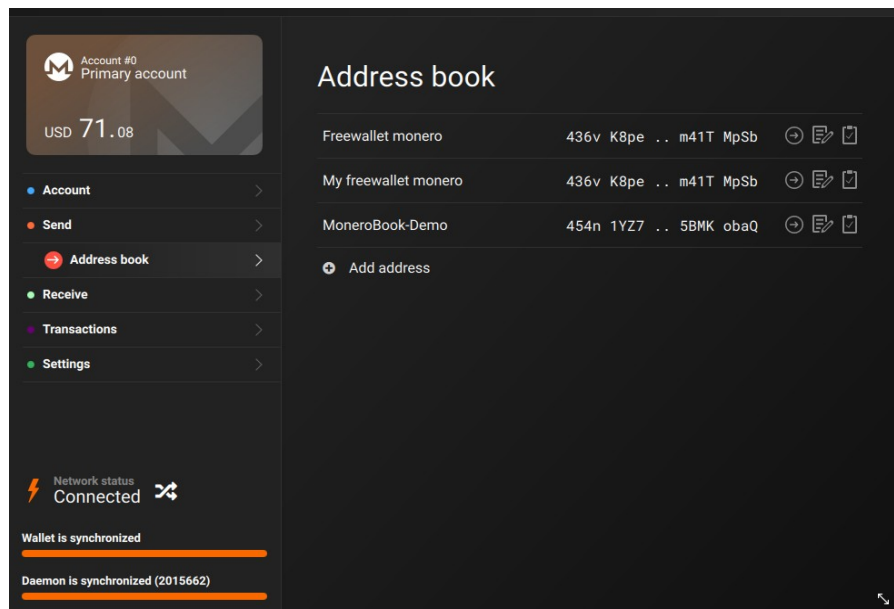
There are two common ways to accept Monero over the Internet. The first is to publish an address that people can copy and paste into their wallets in order to send you Monero. This is a very common approach for websites looking for patronage.

The second is to integrate Monero as a payment method for your website’s shopping cart. To that end, there are plugins available for WooCommerce, Prestashop and WHMCS. These plugins have their own instruction manuals, and configuring shopping cart software is outside the scope of this introductory book. I have had good results with “NoMiddleman Crypto Payments for WooCommerce,” but your mileage may vary, and this is something you’ll need to research thoroughly before implementing in your particular environment.

## Sending Monero

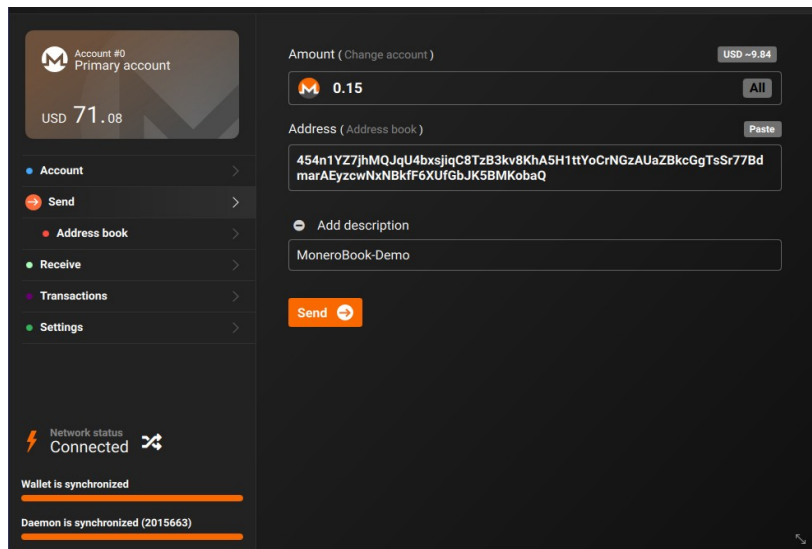
I recommend adding the recipient address to your address book. This isn’t strictly necessary, but it can make things easier.

Next, open the address book, right under “Send” on the left hand side, and click on the arrow just to the right of “MoneroBook Demo.”



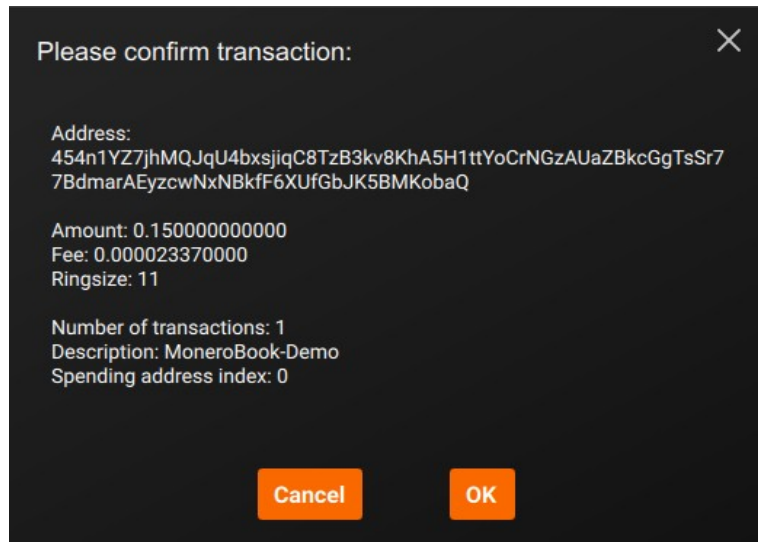
The recipient address is automatically carried over from the address book. Type in the amount of Monero to send – in this case, 0.15 XMR. You can add a description if you'd like, which is kept in your own personal ledger.

Once it looks right, just click the Send button.

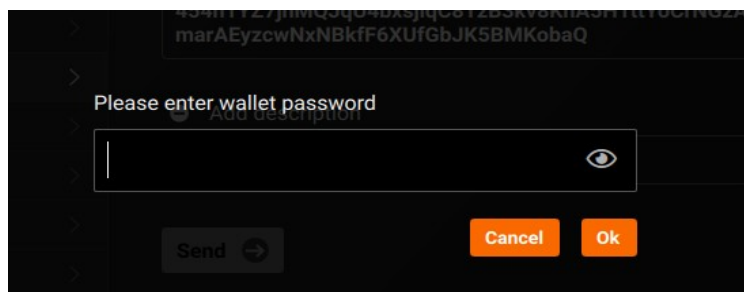


Next, the wallet asks you to confirm the transaction. This gives you a chance to reconsider and make sure everything is the way you want it.

Note that there is a transaction fee to send Monero. For this transaction the amount sent is the intended 0.15 XMR, plus the fee, which in this case is about 0.0000234 XMR, or somewhere between 1 and 2 tenths of one cent.



Last, to authorize the transaction, enter your wallet password. Done!



Looking at the transactions, you'll see that it has a status of "pending" until the ten confirmations have completed.

The screenshot shows a Monero wallet interface. On the left, there is a sidebar with navigation options: Account, Send, Receive, Transactions (highlighted), and Settings. The main area displays the account balance as USD 61.24. The 'Transactions' section shows a list of 9 transactions, with 7 displayed. The first transaction is a 'Sent' transaction of 0.15 XMR, which is currently 'Pending' and occurred 42 seconds ago. The other transactions are 'Received' transactions of various amounts, all confirmed at blockheight 1728020.

Type	Amount	Blockheight	Date
Sent	0.15 XMR	Pending	42 seconds ago
Received	1.08377404 XMR	1728020	400 days ago
Received	0 XMR	1728020	400 days ago
Sent	0.48940708 XMR	1520347	690 days ago
Received	0.5 XMR	1514821	697 days ago

## Taking Monero With You

What if you want to use Monero in circumstances where you aren't using a desktop computer? You'll be pleased to know that there are options available for both Android and Apple phones.

The first option I will mention, because it is easy and convenient, is Freewallet. Freewallet, despite its name, is not a wallet. Rather, it is an app that interfaces to an exchange in Estonia, and that exchange has all the keys. In this sense, it works much more like a regular banking app, and if you were to lose your password to the app, it could be recovered. Unless you try to use the app to purchase cryptocurrency with your bank card, there is also no personally identifiable information – it's all anonymous.

This app allows you to send Monero by scanning QR codes, cut and paste addresses from websites and everything you'd need to do in terms of sending and receiving funds. Although the app works worldwide, the ability to use it to buy with a bank card is restricted to certain countries, and if you happen to live in the U.S., this means you can't use that particular part of their service.

The freewallet app also has a companion website at [freewallet.org](http://freewallet.org) that allows you to track all of the wallets you have with them, and conduct transactions via their website. Overall this is a very convenient service, and I've used it myself.

That having been said – and I will explain more about this in the chapter on exchanges – if you don't actually possess the keys, you don't really control that cryptocurrency. And it's not just about whether or not you trust [freewallet.org](http://freewallet.org) – which has a pretty good track record. Rather, it is understanding that exchanges are prime targets for hacking, and about ten of them are hacked to some degree every year with the sophistication of attacks increasing by the day.

So in practice, if you plan to use Monero via freewallet, send only enough for the immediate transactions to your freewallet address, and no more.

Two other popular real cryptocurrency wallets are Monerujo (Android only) and Exodus (desktop, Android, iPhone). Monerujo is open source, supported by the Monero development community, has an excellent reputation, and a nice interface. It includes QR code reading, send and receive and much more. It also includes a very innovative function that allows you to use Monero to anonymously send to a bitcoin address. Unfortunately, if you reside in the U.S., you can't use that function.

Exodus is a multi-currency wallet that works for all popular cryptocurrencies, including Monero. It offers the convenience of built-in swaps between different cryptocurrencies, a slick user interface, and the ability to use the same account as your desktop wallet (assuming you use Exodus as your desktop wallet as well) by “recovering” the account via the 12-word mnemonic seeds so you would be using the same account whether at your desk, or on the road.

Both of these install automatically via the Play Store or App Store, and walk you through everything step-by-step, so there is no need for me to rehash that here. Instead, I want to point out the obvious: phones get lost and broken. The same cautions that apply to a desktop wallet also apply to a phone

wallet: choose a good passphrase that you won't forget, back up the keys, and write down the mnemonic seed and store it in a safe place. The last thing you want is to be unable to recover funds because you accidentally dropped your phone in a mud puddle.

Furthermore, if you lose your phone, it will have your keys right on it, and the only thing protecting your funds at that point will be your passphrase, so it had better be good! Most wallets, including those I mentioned, are aware of this risk and will automatically lock with the wallet password after only one minute of inactivity.

Meanwhile, wallets are resource hogs because they have to monitor one or more nodes at all times to keep track of transactions. This is a constant active data stream that is trivial on a PC or a laptop, but can run down your phone's battery in a hurry. So I recommend keeping wallets completely closed and off when not in use, or setting appropriate options so this doesn't happen.

(As an aside, one of the most common uses of VPN services is to make it appear as though you are in a different country in order to bypass a variety of restrictions pertaining to watching movies, financial services and so forth. You simply select a server from your VPN provider's menu that is in the country where you want to be located. I would not recommend using your actual bank card for transactions done this way, though. The primary benefit is that it will allow you to see websites that are blocked to the U.S.)

# Exchanges and Coin Swaps

The last two chapters covered how to setup your wallet, and how to use it to send and receive Monero. But most likely, before you can use Monero, you want to buy some with U.S. dollars. In order to do this, you are going to have to use an exchange, and exchanges require a bit of explanation.

In a perfect parallel economy, everyone involved is using cryptocurrency and therefore there is no need for an exchange. I buy my produce from Larry, Larry buys his cow manure for fertilizer from Jake, and Jake pays me for fixing his car. In this scenario, the “dollar economy” is completely cut out of the equation.

But as things currently stand, most things that you need to buy must be paid with U.S. dollars – your rent or mortgage, your income taxes, the grocery store and so forth. So for now, in order for cryptocurrency to have much utility in your life, you need a way to exchange it for dollars. And unless you are getting your cryptocurrency via mining (covered later), the only way you will get it is by either having someone pay you that way, or by purchasing it from an exchange. And an exchange is also the only way for you to turn your cryptocurrency back into dollars.

An exchange is a facilitator between people who want to sell their cryptocurrency for dollars, and people who want to buy cryptocurrency for dollars. The exchange charges a fee, usually between \$1.50 and \$3.00 for this service. By its very nature, an exchange also keeps some liquidity handy – some extra dollars, Bitcoin and so forth to make trades go smoothly.

Exchanges are the “weak link” in cryptocurrency for a number of reasons. For one thing, some of them have been hacked. Some exchanges allow you to keep a wallet that is attached to the exchange, and secured with the password you use to log in to the exchange. When such an exchange is hacked, it is possible for the contents of those wallets to be stolen. Which has happened to more than one exchange.

In another case, and for security reasons to prevent hacking, the exchange owner kept most of the funds of exchange customers in an offline hardware wallet. He died, and was the only one with the password to that wallet, so the exchange had to close with most of the cryptocurrency owned by its subscribers tied up inaccessible in the blockchain forever.

In my opinion, these examples show that you should not keep any appreciable amount of cryptocurrency in an exchange wallet. For my use, I temporarily hold pretty close to the exact amounts needed for a purchase. Balances held in exchange wallets are subject to seizure, forfeiture, and all manner of matters completely outside your control, so they aren't a good place to keep cryptocurrency.

In addition, as the interface between cryptocurrencies and national currencies, exchanges tend to be regulated enterprises and in that respect come to resemble banks. That is to say that most exchanges adopt “know your customer” regulations and require your account to be linked to a verified bank account so that you are clearly and unambiguously identified, and your transactions (and any “gains”) are reported to any interested authorities. In addition, these exchanges will often blacklist and shut down accounts who send funds to addresses known to belong to people with whose politics they

disagree. In other words, they re-introduce a lot of the problems that cryptocurrency was invented to solve.

As an added problem, a lot of people ignored the advice not to speculate on cryptocurrency, and even took out loans on their credit cards to buy into a hype train on cryptocurrency just before it crashed to less than half of its all time high. Banks, already pretty opposed to cryptocurrency, seized that opportunity to justify refusing to allow use of their bank accounts or credit cards in connection with an exchange.

So this means that a lot of banks won't let you use your accounts, even legitimate checking accounts that you have maintained in good standing for many years, to link to an exchange. All you can do is try, and if you fail, find a bank that will allow it.

Unfortunately, many exchanges will not allow you to purchase Monero. Because Monero transactions cannot be traced, they are anathema to corporate exchanges who are merely there to make money off transaction fees, and climb the ladder into big finance in order to become part of the problem, rather than part of the solution.

There are three solutions: 1) peer-to-peer exchanges such as Bisq and LocalMonero, 2) coin swaps such as Changelly, and 3) to ultimately adopt a cryptocurrency-only (and preferably Monero-only) voluntary economy, and thereby cut the exchanges out of the equation.

But until then, exchanges are a necessary evil. So I am going to demonstrate how to use Coinbase, the largest U.S. exchange, to purchase Monero via Changelly, by using Litecoin (LTC) as an intermediary. It sounds complicated, but it is simple.

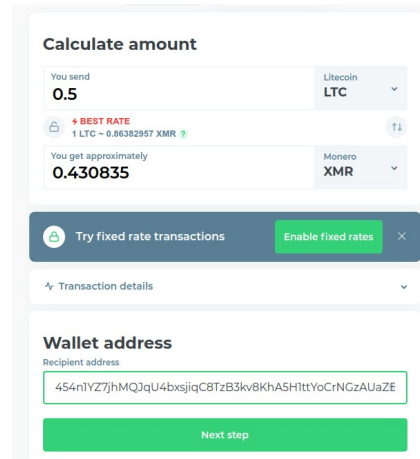
First you need a Coinbase account, complete with all of the Know-Your-Customer stuff such as a copy of your driver's license, a linked bank account and so forth. Set that up according to their directions. (For convenience you'll also need online access to your regular bank account for that to go smoothly.) Go ahead and use your Coinbase account to buy some Litecoin (LTC). I specify Litecoin because it is designed for fast transactions and low transaction fees.

Next, set up an account on Changelly. This costs nothing, and requires only an email address. If you want, you can use Protonmail or a similar anonymous email provider. Once these accounts are set up, you are ready to put some Monero in your wallet.

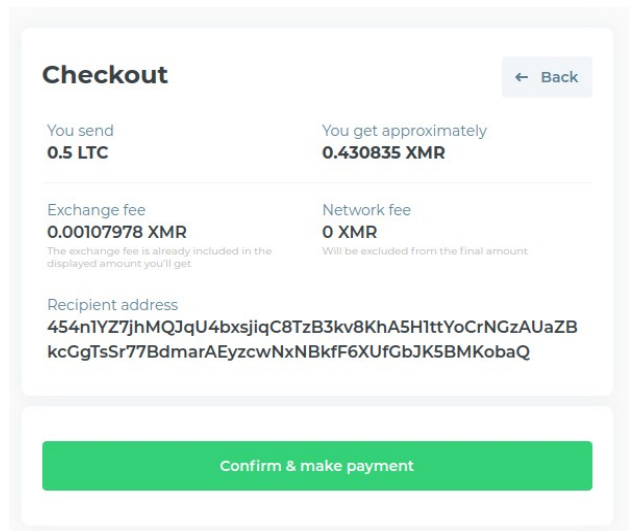


## Obtaining Monero

Start with logging in to your Changelly account, and initiating an exchange. Please notice that I have specified that I am going to be sending LTC, and that they will be sending me back XMR. I have specified 0.5 LTC, but you can use whatever amount makes sense for you. Also notice at the bottom that I have entered the address of my Monero wallet as the recipient. After all of this looks good, click on “Next Step.”

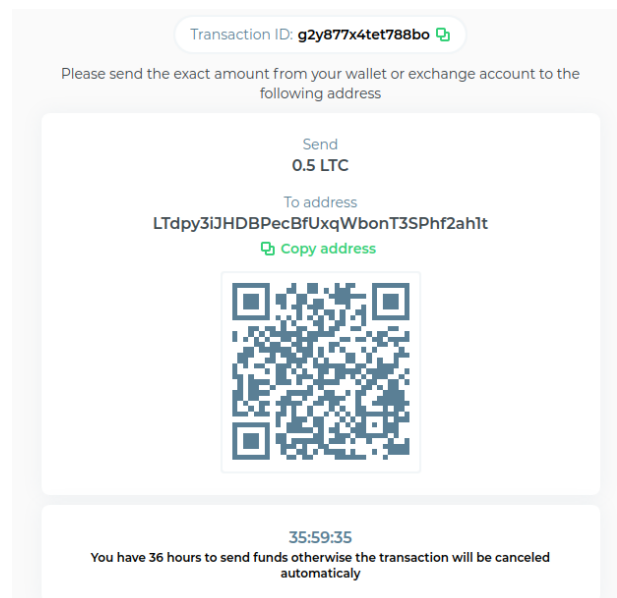


The Changelly website reflects your intended transaction back to you, and asks for you to confirm it. Go ahead and click “Confirm and make payment.”



Changelly now gives you a one-time use LTC address. Highlight this and copy it into your clipboard or just click “Copy address.”

Leave the Changelly site open in one browser tab, and then open your Coinbase account in the other. (Coinbase uses “two factor authentication” and may text you an SMS code in order to log in.)



After logging into Coinbase, select the options to send LTC from your balance to another wallet, and you will get a pop-up box that looks like this.

Enter the LTC address that Changelly provided, and the exact amount of LTC (in this case, 0.5 ) that you committed to send.

When everything is ready, click “Continue.”

The screenshot shows the 'Send LTC' interface. At the top, there are tabs for 'Wallet Address' and 'Email Address'. A note states: 'A network fee will be added for sends to LTC addresses. Network fees do not go to Coinbase. To avoid network fees, send to an email address. Learn more.' Below this is the 'Recipient' field with the address 'LTdpy3iJHDBPecBfUxqWbonT3SPhf2ah1t'. The 'Available to send' section shows '0.6601 LTC = \$38.05'. The 'Amount' section shows a conversion from '28.82 USD' to '0.5 LTC'. There is a 'Note' field with the placeholder 'Write an optional message'. At the bottom is a blue 'Continue' button.

Coinbase will send you an authentication code via SMS, to make doubly-sure that it is really you sending the funds.

So enter that code, and click “Confirm.”

The screenshot shows the 'Confirm LTC Send' interface. It features a 'Transaction Details' table:

Transaction Details	
To	LTdpy3iJHDBPecBfUxqWbonT3SPhf2ah1t
Amount	0.5000 LTC \$28.82
Coinbase fee	\$0.00
Network fee	0.0000042 LTC \$0.00
Total	0.5000042 LTC \$28.82
Note	

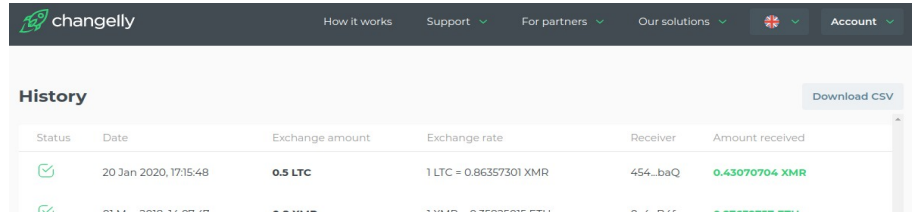
Below the table, it says 'Enter your 2-step verification code' and shows a field with the code '495729'. There is a link 'Didn't receive the SMS? Re-send SMS'. At the bottom are 'Go Back' and 'Confirm' buttons.

Coinbase then confirms that everything went as planned.

Go ahead and exit Coinbase, and return to your Changelly tab, and select the option under your account to look at your history.

The screenshot shows the 'Send Complete' confirmation screen. It features a large green checkmark icon and the text: 'Your transaction is on the way! You sent 0.5000 LTC (\$28.75) to an external address.' At the bottom is a blue 'View Details' button.

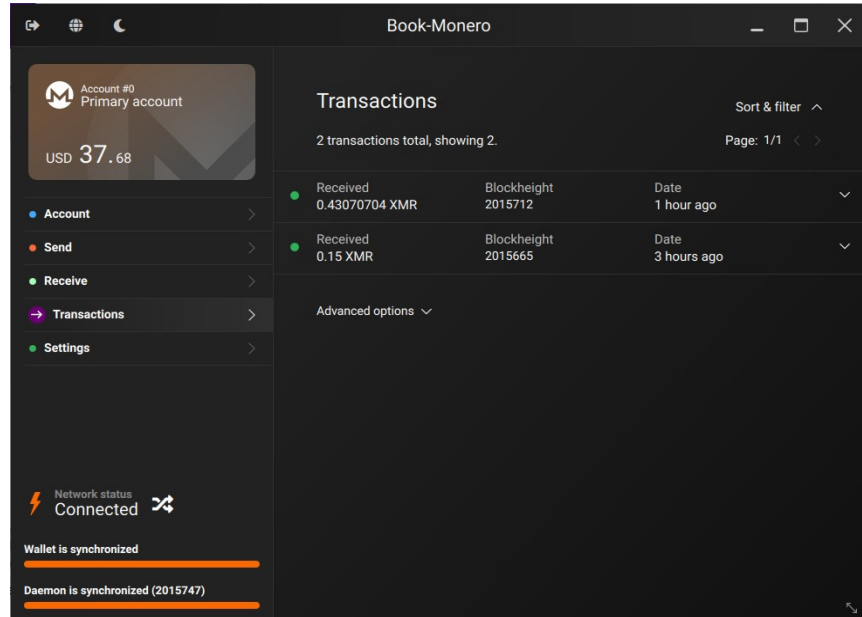
In about twenty minutes, the history for your account on Changelly will reflect receipt of your payment in LTC.



The screenshot shows the Changelly account history page. The header includes navigation links: "How it works", "Support", "For partners", "Our solutions", and "Account". The main heading is "History" with a "Download CSV" button. Below is a table with the following data:

Status	Date	Exchange amount	Exchange rate	Receiver	Amount received
	20 Jan 2020, 17:15:48	0.5 LTC	1 LTC = 0.86357301 XMR	454...baQ	0.43070704 XMR

Next, open up your Monero wallet to look at your transactions. You will see the Monero deposit right ahead of the earlier 0.15 deposit we used as an example. Now you have Monero in your wallet that you can use to buy things, as described in the previous chapter.



The screenshot shows the Book-Monero wallet interface. The top left displays the account balance: "Account #0 Primary account" with "USD 37.68". A sidebar menu includes "Account", "Send", "Receive", "Transactions", and "Settings". The main area is titled "Transactions" and shows "2 transactions total, showing 2." The transactions are:

Transaction	Blockheight	Date
Received 0.43070704 XMR	2015712	1 hour ago
Received 0.15 XMR	2015665	3 hours ago

At the bottom, the interface shows "Network status Connected" and "Wallet is synchronized" and "Daemon is synchronized (2015747)".

If someone has paid you some Monero and you want to put your Monero into an exchange so you can extract it via your bank account, you simply reverse this process and use the address of your exchange LTC wallet as the recipient, and initiate an XMR to LTC trade.

Earlier in the chapter I mentioned Bisq, a peer-to-peer exchange. This is my preferred option because it completely eliminates the use of places such as Coinbase. The problem is that it has a reasonably steep learning curve. While you are just beginning, it is best to stick with the big and well-known exchanges with a good track record, such as Binance, Coinbase, and so forth. Once you have built a comfort level dealing with these things, then feel free to use the more advanced peer-to-peer option, which also has the advantage of respecting your privacy, and leaving no records.

## **Bypassing the System: Local Monero and Bisq**

As previously mentioned, exchanges are the “weak link” in cryptocurrency because they re-introduce a number of the problems that cryptocurrency was intended to solve. Despite this, I recommend that people who are new to cryptocurrency use such exchanges (e.g. Coinbase, Binance, etc.) because they are simple and as long as you follow the foregoing instructions, the privacy of your transactions is still relatively assured.

But they are also a weak link in other ways. For one thing, they can be shut down by government decree at the stroke of a pen, as happened in China. This is not a comforting thought, particularly if you need to exchange cryptocurrency for dollars in order to pay bills and your exchange just got shut down.

The next level up in exchanges are so-called “peer-to-peer” exchanges. The two I will discuss here are LocalMonero and Bisq.

### **Bisq**

Bisq is focused on Bitcoin, but because you can use it to buy Bitcoin without a paper trail, which can then be used to buy Monero, it is a worthy subject. It is also important because the entire thing is decentralized.

Bisq runs on peer-to-peer software with no centralized servers. There are a few of these, but the premier exchange of this type is Bisq. Through a number of mechanisms, Bisq is secure, private and censorship resistant. But before you can use Bisq, you have to already have some Bitcoin, which means you will “seed” it by transferring some Bitcoin from a standard exchange such as Binance or Coinbase.

Before diving into the nuts and bolts of dealing with Bisq, I want to explain what a peer-to-peer exchange does.

Standard centralized exchanges are like exchanges for stocks, keeping a bit of crypto handy as well as national currency and they facilitate exchanges “on the fly” by working in an aggregate way, so that the cryptocurrency you buy didn’t come directly from one individual who sold it. This makes transactions easy, fast and convenient. For this service, they charge a fee for each transaction.

Peer-to-peer exchanges work more like an online auction site where people looking to buy and people looking to sell post what they are looking for, and two distinct individuals make the trade. That is, instead of buying from an exchange, you are buying from a specific person. The exchange itself has no idea who you are, or where you are. The only people with any knowledge of the participants in a transaction are the participants themselves.

So far, so good, but what happens if you hand someone U.S. dollars, and they don’t deliver what they promised? There are a number of mechanisms to prevent and deal with these problems, including

trading limits, bonding, escrow and mediation. Each exchange handles these somewhat differently, but these will all be explained within the context of Bisq.

Bisq has no centralized server. It is a peer-to-peer system similar to a distributed “help wanted” section, where your personal information is only on your own computer. When you first download and install the software, it creates a Bitcoin wallet for you that is integrated with the software. You should take that opportunity to click the menu item to set a password (otherwise anyone with access to your computer can access the wallet), and also click the menu item to get your wallet seeds which you will store in a safe place, so you can recover the wallet if needed.

Likewise, click on the “Account” menu item, and then “Funds” so you can copy and paste your Bitcoin reception address. Save it in a text document, because you will need it later.

Next, set up your “National Currency” accounts. You can set up accounts of various types: Western Union, Moneygram, Zelle, Postal Money Order, in-person cash, and more. The key here, and this is important, is that you MUST specify these accounts using the exact same information as will appear to anyone receiving the funds.

When you send money via Western Union or Moneygram, they check your ID and make sure the sender information on the form is identical to your ID. A Zelle account is verified by connection to an existing bank account. When the recipient gets the funds, Bisq protocol specifies that they refuse the funds if the data does not exactly match what was conveyed to them from your setup in the corresponding National Currency account.

You will find that most offers on Bisq for selling Bitcoin are in exchange for Zelle. Zelle is a service offered by a cooperative of the largest U.S. banks that allows for transfer within the country between any people with domestic bank accounts. It competes with services such as Western Union domestically, and has far lower fees. The transfer is nearly instantaneous, and has a very low risk of chargeback, unlike services such as Paypal. (I’ll explain why this is an issue shortly.)

After your National Currency accounts are set up, click on the tab to set up your “altcoin” accounts. This is where you put the receiving address for your Monero wallet. In the Bisq system, at least one side of each transaction must use Bitcoin, but you can use Bitcoin to buy Monero or other cryptocurrencies.

Now there is one final step to get started: go to your regular cryptocurrency exchange, and buy about \$50 worth of Bitcoin. After that is complete, send the Bitcoin to the Bisq Bitcoin wallet address that you saved earlier. This will be used for bonding and to cover fees.

## **Keeping Things Honest**

Bisq is a very technically solid platform using the latest end-to-end encryption and its own well-designed protocols. But its real genius lies in how it has addressed the human problems.

Practically every day of our lives we are beset with scams from all sides: emails purporting to be from our bank or ISP “verifying” our passwords, robocalls from fake charities asking for a credit card

number, phone calls allegedly from the IRS demanding immediate payment to avoid jail, identity theft powered by hacks of our social security numbers from major credit unions or our personnel records with the federal government, and even fake employment schemes. And who among us hasn't had their bank card shut off by the bank because, somehow, it was being used to purchase luxury items on the other side of the world? Schemes, scams, fraud and theft have become so pervasive that we now accept them as part of the background noise.

So how, in such an environment, can anonymous people exchange cryptocurrency without being ripped off? How can you send a postal money order to some address, and be confident that you will actually get the Bitcoin you expect?

Bisq has a variety of mechanisms in place to account for the human factor that, in aggregate, make fraud and scams relatively rare.

The first is account aging. There are limits to how much you can buy with a given national currency account based upon how long it has been in use. Its "aging" starts from the first time it is used. So an account that has newly been set up has lower limits than an account that has been in use for a month or two months.

The second is that limits are applied to the various methods of payment based on charge-back risk. Most people have done a charge-back without ever considering its more devious possibilities when calling the bank to dispute a charge for an item that was paid for but never received. But what if you purchased something like gold, took possession of that gold, and then called your bank to tell them you had never received it? If the bank believed you, they would reverse your payment to the seller, and now you would have both your money and the gold!

Although such scams aren't common when people are buying standard goods and services, they are a huge problem when dealing with assets readily convertible to cash, including cryptocurrency. As a result, most sellers of cryptocurrency will not accept forms of payment with readily reversible transactions, such as credit cards. Payment methods accepted in the Bisq network are those with a low risk of reversal such as Zelle, Postal Money Orders, Western Union and so forth. The higher the risk of reversal, the lower Bisq sets the limits on that method of payment.

The third is timing. Depending on the agreed-upon payment method, each transaction has a specified period of time to be completed. The buyer sends payment as soon as possible, and the seller acknowledges payment near the end of that period. This period is long enough for the funds to be safely in the seller's bank account with a low risk of reversal. After this is a special 10-day count-down timer that I will explain later.

The fourth is that buyers must post a bond in the form of a certain amount of Bitcoin as a promise that they will send the specified payment. If the seller doesn't acknowledge payment by the end of the transaction period, the bond is forfeit and is used by the Bisq network to help pay its developers. If the transaction is successfully completed, however, the Bitcoin bond is returned to the buyer's Bisq wallet. In addition to posting the bond, the buyer also pays a small transaction fee. Transaction fees go to pay bonded arbitrators.

Why would a buyer refuse to send payment? The general scenario for this is that the price of Bitcoin dropped after the transaction was agreed to. As a result, the buyer no longer considers the transaction to be a good deal, and wants to back out. Posting a bond makes this scenario less likely.

The fifth is multi-signature escrow. When a transaction is agreed upon, the seller puts the contracted amount of Bitcoin into an escrow account. That Bitcoin is automatically released to the buyer's Bisq wallet once the seller acknowledges receipt of funds.

What happens if the time limit elapses for the transaction, you can demonstrate that your funds have been received, but the seller has not acknowledged receipt? First off, the ten-day countdown timer starts. At the end of that ten days, if nothing happens to prevent it, that Bitcoin is released to you automatically. This puts time pressure on the seller to resolve any dispute.

Why would a seller do this? It could easily happen if, during the time period for the transaction, the price of Bitcoin in dollars had doubled. In such a case, the seller would rather hold on to the Bitcoin than keep the agreement.

Of course, this sort of situation is a dispute, and the Bisq software allows you to click a button to engage a mediator to assist resolving the dispute. It could be as simple as the seller being sick in bed, or as serious as intended fraud. If the mediator's suggestion is accepted, then the transaction proceeds accordingly. But if it is not accepted, the matter goes to arbitration.

Arbitrators are bonded members of the Bisq community whose services are paid via transaction fees. They have the ability to sign the multi-signature Bitcoin transactions, and send disputed funds to your wallet.

Although I've only hit the high spots and there are a lot more details to how these processes work, this explains the key mechanisms that Bisq has used to make fraud rare within the network. But it also highlights the importance of keeping all documentation for payments until a transaction is complete.

## **Disadvantages of Bisq**

If you are looking to drive a nail, you might try to use a wrench as a hammer. Bisq is a low volume exchange intended to facilitate person-to-person transfers. Transactions, depending on how you do them, can take hours or even days. Furthermore, transaction limits are relatively low compared to the big centralized exchanges.

This makes Bisq wholly unsuitable for people trying to churn Bitcoin in order to make money on momentary ups and downs. Anyone attempting to be a day trader will be entirely unsatisfied with Bisq.

Although Bisq knows nothing of your personal details, those with whom you conduct an exchange will know everything about you that is attached to the public side of your National Currency account. That is to say that, like anyone from whom you purchase things over the Internet, they will know your name, address, email address and phone number of record.

Because privately exchanging cryptocurrencies is not illegal, I am perfectly comfortable with this. I think it is a small price to pay for being able to completely bypass any records of purchase or ownership of cryptocurrency. But if you are not comfortable with it, Bisq is not a good platform for you.

In my opinion, you should also avoid the “cash in person” payment methods for the rather obvious reason that undertaking such activities using cash with strangers is just begging for trouble. There are ways to do it safely, and the Bisq website has some good tips, but this is a book on cryptocurrency rather than self-defense.

## **Let’s Buy Some Bitcoins!**

Despite all of the previous explanation, in practice, buying Bitcoin via Bisq is simple. Set up an account on Zelle, use that Zelle account as your National Currency account on Bisq, and then accept an offer to sell Bitcoin in exchange for Zelle.

Over half of the banks in the U.S., and all of the big ones, are already partnered with Zelle and you can set up Zelle right in your bank’s mobile banking app on your phone. Go to the Zelle website, and click on the name of your bank for instructions.

If your bank is one of the rare ones without a direct interface, you can set everything up right on the Zelle website, following their instructions.

Once that’s done, set up Zelle as a National Currency account in the Bisq interface. You should have already funded \$50 worth of Bitcoin in your Bisq wallet as instructed earlier.

Now, click on the “Buy BTC” button to review available offers. Only offers that match your payment methods will be available for selection. Follow the directions and ... it’s as simple as that. Once you have the Bitcoin, you can use it to buy Monero, either via Bisq or via other means.

## **Keeping it Local: LocalMonero**

Most of what I previously discussed about Bisq applies to LocalMonero.co. (That’s the correct spelling of the URL.) The primary differences are that LocalMonero runs on a centralized website rather than peer-to-peer software, and that the predominant payment methods are coins such as Litecoin(LTC) rather than Zelle. You’ll recall from the previous chapter that I advocated using LTC as an intermediary in Monero conversions.

Like Bisq, there are escrow requirements and multi-signature wallets in order to avoid ripoffs. LocalMonero is a great way to convert LTC from a regular exchange back and forth with Monero, but being a centralized site it lacks the censorship resistance of Bisq.



## Internet Resources

Newsflash: Google and its Youtube subsidiary try to transparently censor cryptocurrency content in general, and a lot of the most useful websites pertaining to Monero do not show prominently in web searches. Here are some sites you want to know about, and that you'll find if you use the English version of the Russian Yandex search engine.

### Monero.how

This website contains about 50 up-to-date tutorials on every aspect of Monero from using wallets and cold storage to using peer-to-peer exchanges.

### Localmonero.co

Please notice that the end of that is co, not com. This is the premier person-to-person Monero exchange that allows you to buy and sell Monero in exchange for other cryptocurrencies, Western Union transfers, and even cash.

### Bisq.network

Bisq is primarily a peer-to-peer Bitcoin exchange but it features very impressive privacy controls by virtue of its decentralized model. As long as one side of a transaction is in Bitcoin, the other side can be in any other currency, including Monero. This is an excellent place to purchase cryptocurrency, generally using Zelle interbank transfers, without leaving any records that would exist on the big exchanges.

### Morphtoken.com

Until recently, shapshift.io handled conversions between other cryptocurrencies and Monero. In this book, I illustrated using changelly.com for that purpose. But how long before that becomes a problem too? Morph Token anonymously handles conversion between Monero and other popular cryptocurrencies such as Ether, Bitcoin and Litecoin.

### Getmonero.org

The primary distribution site for the official Monero wallet.

A number of these sites also have .onion addresses that can be used via TOR – which is something I'd encourage for privacy reasons.

## Conclusion

Hopefully this booklet helped make cryptocurrency more understandable, and you now see why cryptocurrency exists, and what makes Monero such a special currency that you should use and support.

At this point, you should now have a fully funded wallet available to you.

This is a relatively short book, but my intention was to give immediately actionable information, and it is my sincere hope that I have done that! Welcome to the world of Monero – a world where your transactions are your own business, and nobody can decide at random that you aren't allowed to buy something, simply because they don't like your opinions.

And while you are at it, you should strongly consider joining European Americans United. It costs you nothing, and the more people we have, the more we can do.

And speaking of doing things, what we can do is determined to a large degree by our finances. Whether you join us or not, if you are feeling generous and want to test out your brand new Monero wallet, you should go to our TOR hidden page, and send us some Monero!