

# The Idiot's Guide to Bitcoin



By Gustaf van Wyk



# The Idiot's Guide to Bitcoin



Gustaf van Wyk

---

All Rights Reserved

---



---

**Disclaimer:**

The material in this publication is of the nature of general comment only, and does not represent professional advice. It is intended to provide specific guidance for particular circumstances and it should not be relied on as the basis for any decision to take action or not to take action on any matter which it covers. Readers should obtain professional advice where appropriate, before making any such decision. To the maximum extent of the law, the author and publisher disclaim all responsibility and liability to any person, arising directly or indirectly from any person taking or not taking action based upon the information in this publication.

# Contents

Foreword	-	<i>i</i>
About this	-	<i>iii</i>
Start here	-	<i>v</i>

## Part 1 - MONEY

Chapter 1 -	What the Heck is Money, and Why Doesn't Anyone Care About it During a Zombie Apocalypse?	1
Chapter 2 -	Our Current Monetary System, Paper Currency, Centralized Banking and Debt.	12

## Part 2 - BITCOIN

Chapter 3 -	WHAT IS BITCOIN	
	• How Bitcoin is changing the World	23
	• What is Cryptocurrency	24
	• The Rise of Bitcoin	26
	• Legitimacy	27
	• Decentralization	28
	• It's like Gold, but Better	30
Chapter 4 -	HOW BITCOIN WORKS	32
	• Bitcoin Creation	33
	• What can Bitcoins be used for	34



Chapter 5 - BUYING & SELLING BITCOIN	
• How it's Done	37
• The Bitcoin Wallet	38
• Paper wallets AKA "Cold Storage"	39
• Software Wallets	42
• Mobile Wallets	44
• Web Wallets	45
• Transferring Bitcoins between Wallets	46
• Buying Bitcoins	47
• Bitcoin Exchanges	48
• Selling Bitcoins	55
Chapter 6 - TRADING BITCOIN	60
• The Bitcoin Economy	61
• The Psychology of Trading	63
• Bitcoin Trading Basics	66
• Live Bitcoin Market Charts	67
• Helpful Mobile Apps	70
• Forums and the Bitcoin Community	71
• Set your alerts and search for Info Daily	72
• Buy Low, Sell High	72
Chapter 7 - SPENDING, ACCEPTING AND PROMOTING BITCOIN	73
• Spending Bitcoin Online	75
• Donating Bitcoins	75
• Spending Bitcoins Offline	76
• Accepting Bitcoins as a merchant	76
Chapter 8 - MINING BITCOIN	
• Thar' be Gold in Them thar' Hills!	82
• How Mining Works in a Nutshell	83
• Bitcoin Mining Hardware	85
• Bitcoin Mining Software	87
• Mining Pools	88
QUESTIONS & CONCERNS	
• I'm Afraid Bitcoin will be hacked - everything can be hacked!	89
• Will The Government Shut Down Bitcoin?	91
• Is Bitcoin Just a Bubble Waiting to Burst?	92
CONCLUSION	95

---

## Foreword

The 'Idiot's Guide to Bitcoin' provides you with an integral understanding of the digital currency known as Bitcoin which is revolutionizing the way we think about money. It explains everything you need to know to get involved, from beginning to end.

Though this book is part of a larger movement towards economic freedom it focuses absolutely on making Bitcoin easy. At first glance digital currency might seem like a small and exclusive movement on the internet that might not have uses beyond those of today's laptop-investors and cyberpunks. The 'Idiot's Guide to Bitcoin' aims to demonstrate how important this change in the way we think about money is and most of all to show you how easy it is for you to get involved.

The book starts by discussing the main principles of Bitcoin as well as some of the more politico-economic implications of the revolution. These are covered in depth but the book is designed in such a way that these can easily be skipped in case you are more interested in getting to the nitty gritty of things right from the start. There are some technical parts to understanding Bitcoin and the book covers these in an easy to follow, step-by-step fashion. There are ten chapters in all and every chapter covers a different aspect of Bitcoin in the most appropriate fashion. Nothing is left out.

The implications of a Revolution, and Bitcoin IS a revolution, is often uncertain and shrouded in rumour and conjecture. The Idiot's Guide to Bitcoin deals with all the concerns surrounding Bitcoin on a factual basis and strives to inspire confidence in you by giving you a sound understanding of everything Bitcoin and provide you with resources that you can turn to when in doubt.

I wrote the Idiot's Guide to Bitcoin with you in mind. I've tried to best support the Bitcoin movement by making it easy and accessible for everyone. I want you to experience firsthand, as I have, the benefits of Bitcoin as a currency as well as a commodity. I wanted to show you the freedom that Bitcoin offers and that the returns are nothing short of magnificent. I wanted to be the one to introduce you to our future! So I wrote the Idiot's Guide to Bitcoin.

What you read in these pages could set you free and give you confidence that the future of global economics is not dire. Not to mention the financial gains that stand to be made as the relative young economy grows and its value increases. So I encourage you to grab this opportunity with both hands and join us in making the world a freer and wealthier place for everyone.

Wishing you freedom and prosperity

Gustaf van Wyk

## About this...

**A**lmost two years ago I was made aware of Bitcoin as an anonymous way to make payments. At the time Bitcoin's value as a means of exchange seemed to be very much linked to the clandestine depths of the internet. It's was trading at below \$10 for one and didn't look like much but on that fateful day the larger implications of Bitcoin dawned on me.

I have always maintained a strong philosophical approach to life and as such have resolved to stand for that one and only absolute right of man that is freedom. I had been aware of the dictatorship-like form of the global financial situation for a long time. Centralized banking is a curse on modern life, a poorly disguised form of good ol' slavery in the form of self-perpetuating debt and everybody knows it, right. Yet despite a pervasive awareness of its oppressive nature, we-the-people are still ruled by and subject to these powers. It still surprises me how seldom these accusations are taken seriously, and when they are, they are very easily dissolved, discredited or destroyed by those that guard and maintain the apexes of power. So fighting the fight on the ground just isn't, and will never be effective. Not as long as they have us by the wallet. It would be far more effective to just find and implement our own solution that works immediately and circumvents politics which as you know is far more self-serving than it is service-providing. I realised in a moment that Bitcoin offers just such a solution.

Bitcoin threatens to make obsolete a system of power that is aggressively defended by those that wield its sceptre but my book, the Idiot's Guide to Bitcoin, was not written in defiance of the corrupt but rather in support of the free. Bitcoin is a modern solution to an old problem. If money is power then Bitcoin gives it back to the people. Should Bitcoin ever become globally accepted as a mainstream way to safely and freely

make payments then mankind will take a revolutionary step, a leap forward into the next chapter of civilization. We would expel the use of force from our economies and embrace free and volitional exchange, as trade was meant to be. Something the founding fathers would be proud of.

I believe absolutely in the potential that concepts like Bitcoin and decentralized currency have to change the world as we know it, and I am not alone. Every day the revolution grows. When I look at history and see the progress we've made from medieval to modern, I can't help but feel that progress in the right direction is inevitable despite the best efforts of the corruption in man. Freedom is inevitable it's just a matter of time. Bitcoin, if nothing else, is a step in the right direction. The Idiot's Guide to Bitcoin is a gesture in support of the movement.



# Start Here

## Just a Quick Note Before we get Started

**Part I** of this book is about money and the problems that modern financial systems pose to us as a civilisation. It exposes the problem to which Bitcoin is a solution. It is a good place to start if you are interested in the politico-economic implications of Bitcoin. However, if you are unconcerned about all that jazz and want to get right into Bitcoin and understanding how to buy, sell, trade, spend, mine and promote Bitcoin then skip straight to **Part II** on page 23.

**Part II** is the in-depth step-by-step guide that the title of this book promises to be.

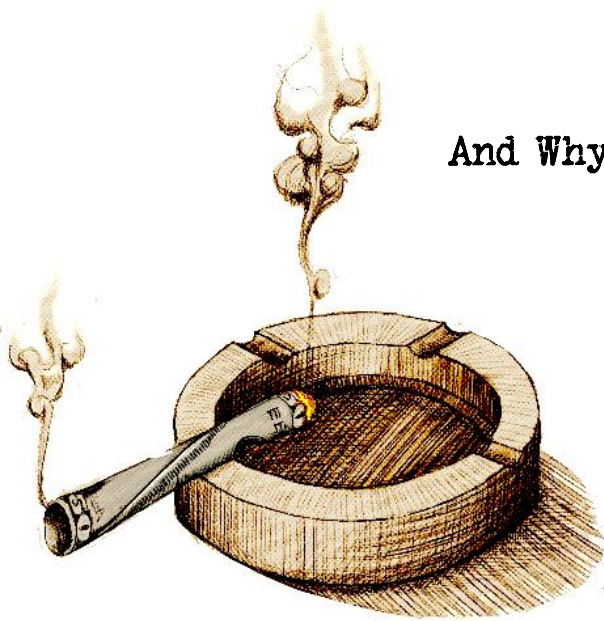
Enjoy!

# PART 1

## What the Heck is Money, And Why Doesn't Anyone Care About it During a Zombie Apocalypse?

---

(Chapter 1)



**F**rom the minute we're born until the minute we die, one thing is always principal on our mind – money. Without it we can't have a roof over our head. We can't put food in our mouths. We can't move from point A to point B. We are driven through formal education from grade school to high school to college to corporate training and beyond so that we may find a suitable career in life in order to trade our time and services in exchange for money. When we're not busy making money or complaining about the job we hate, we're out spending money and complaining about how broke we are – well at least around 97% of us are.

---

Money has become nothing more than numbers on a screen or pieces of paper in our pockets. It's not so much what the money is or what gives it value that matters to us, only how much of it we have versus the amount various institutions are trying to take away from us (utility bills, debts, taxes). The value of money is a no brainer for us because it's always been there in the same exact form since we were born. Most of us understand that the value of our money can waver through inflation and market trends, and that costs of things can rise, but still we go on accepting that this money we use is the only way to pay for things. So, we go on without questioning really where it comes from or of what value it really is.

If you really stop to look at money, it's kind of terrifying in a really interesting way. You see, that money you spend – that you base your entire life around, that you literally cannot live without – is backed by absolutely nothing except your faith in it. That's right – the money you have really is just pieces of paper (often times not worth the paper it's printed on) and it really isn't anything more than numbers on your screen. It's even more terrifying when you realize that a small, private group of individuals control the value of your money and how much of it is in circulation.

In effect, all of the world's currency and how we place value on things is completely made up, and the reason it was made up in the first place was to replace the annoyance and inconveniences of bartering (we'll get into that in a minute).

Essentially, if the zombie apocalypse breaks out tomorrow and a bunch of undead, flesh-eating shells of former human beings were hobbling around empty-eyed bent on consuming your brains, and you were the world's richest human being with billions of dollars in your digital bank account, and you offered someone with a zombie-proof bunker stocked with enough food to last at least 20 years all of that money to let you in, they wouldn't care. Why? Because your money is valueless at that point. It's the zombie apocalypse for cryin' out loud, what value does money have?

That is essentially how money of any form works – it's only worth the amount of faith that people have in it. During the zombie apocalypse,

society as we know it has been crippled therefore money as we know it holds no value because no one has faith in it anymore. In fact, at that point, gold holds no value, fancy paintings hold no value. The only thing that holds any value are the most tangible assets – food, shelter, water, and protection (guns, ammunition). Of course, you could go the Mad Max route and add in gasoline as a staple currency, but it all works out about the same – all those dollars and euros and pounds won't be worth squat.

This is how the world began and before there was any concept of money, the only value we put on things were how they would help us survive. Without going into a painful history of the world, evolution, and the ascension of finance, let's just pummel through it like a five year old kid with ADD who just ate an entire batch of brownies and washed it down with a Red Bull. Ready? Let's go! (Oh look, a bird!).

Okay – back on track. Mesopotamia was one of the world's first civilizations and was clustered with a few others that began appearing about 5,000 years ago along near what is now the Tigris-Euphrates river system in the Middle East. Although it is by far not the first civilization to begin trading (mankind has been using agriculture and trade for about 10,000 years) it is among the first to start keeping records with a written language.

Back then people used clay tokens to record transactions that involved agricultural produce such as barley and wool as well as precious metals like silver. Silver, right along with things like grain, served as money because they held value. However, it was the clay tablets themselves that were more important. The funny thing is, one of the primary reasons the Cradle of Civilization began a written system wasn't to write history or poetry or philosophy, but to record business transactions.

Many of these small clay tablets are preserved even more so than ancient coins post-dating the tablets. They have inscriptions stating things like the bearer of the tablet will receive a specific amount of barley at harvest time or that the bearer should be given a particular amount of silver at the end of a journey.

This sounds pretty familiar to many of us, because they're not much different than bank notes. For example, the words on the Bank of England bank notes read, "I promise to pay the bearer on demand the sum of X." You see, the banknotes (which actually originated in seventh-century China) are not, in and of themselves, worth anything at all. The clay tablets upon which these inscriptions were written were not worth anything. They were just recorded promises on behalf of the person who issued it that, when the time came to turn in the tablet or "promissory note" as the Western designation goes, they would receive something of actual value (grain, barley, a bunch of goats). Therefore, this "money" was backed by tangible assets.

This type of payment system was a more refined way to barter. In fact, even today, we're still bartering – we exchange time and services for money, which then allows us to purchase things we need in order to survive. This isn't much different than what was done for thousands of years – I grow a field of corn, and take the corn to a man who raises cattle to exchange a certain amount of corn for that cattle. That man then takes my corn and exchanges it for horses to herd his cattle. The problem with that bartering system, however, is what if no one needs my corn because they already have enough? Then suddenly the only commodity I have to barter with is useless. This is where precious metals as a form of currency comes into play.

Money – in any form (dollars, gold, or sea shells) is a form of exchange, which carries the advantage of getting rid of the inefficiencies of barter by supplying a unit of account that will facilitate valuation and calculation, and a store of value, that allows for transactions to be conducted over long periods and geographical locations.

People needed a more convenient way to purchase any item– a sort of universal "thing" that could be exchanged for goods and services. What that "thing" is must hold value equal to the goods or services being offered and in order for something to hold value it must be rare and scarce. Let's talk about that for a second.

If I lived by a fresh water stream with an endless supply of pure drinking water in a forest surrounded by wild game and soil perfect for growing

anything I wanted, and I built a society in this area, then we would have an abundance of everything we could ask for in order to survive comfortably. If everyone had ready access to all of this and it was free for the taking because it was so abundant, then I would want for nothing. In the same sense, if money actually grew on trees (as the saying goes) then that money would be absolutely worthless. Oh, you're going to pay me money to wash your car? Never mind then, I have three money trees growing in my yard, why on earth would I do anything for you in exchange for such a useless, petty thing as money?

In order for anything to be worth an exchange, another person has to be without it – you have to have something I want, and I need to have something you want, therefore we barter and exchange goods/services. In the same sense, in order for a universal or even regional currency circulated within any population to be worth something, that currency must be something people desire. Desire for something only comes when it is rare and not readily abundant.

Pearls are worth a lot because they are so rare – it takes an oyster ten to twelve years to develop a pearl. Of course, then you have to be lucky enough in order to find that oyster with the pearl. Because of its extreme rarity, it is desired, and because of that it can be used in exchange for just about anything. Gold and silver is only developed in certain places and must either be panned or mined. The same thing goes for rare gemstones, plants, medicines, and so on. There are many ancient island nations that used certain types of clam shells as currency – if society placed worth on it, it could be used as a means of exchange.

Therefore, currency can literally be ANYTHING that is rare, scarce, and desirable. Currency doesn't even have to be a physical thing – it can be knowledge. If I know where something valuable is, my knowledge of that could be used as currency (I won't tell you, unless you pay me first – perhaps with a promissory note or clay tablet guaranteeing me X amount of things once I reveal the location of the treasure). Currency can also be things like physical labor.

In this same way, one man's junk is another man's treasure. If I live in a location where gold literally pops right out of the ground and it's nothing



new to me, and it's just everywhere, then it's not worth anything to me. However, if someone happens upon where I live and gold is extremely rare where they're from, they'd probably be amazed at how rich I was – they wouldn't understand that I don't care about the gold, and I wouldn't understand why they were so obsessed with it. So you see, value is fleeting and is dependent upon a numerous amount of factors and situations, the primary of which are scarcity and demand.

The above example is taken from real world situations – Pizarro and the entire Inca civilization for example. Five hundred years ago, the most sophisticated society in South America was the Inca Empire – they also had zero concept of money regardless of the fact that they had gold hanging from their ears, noses, necks, wrists, and ankles. They had gold chairs and buildings and plates and bowls – heck gold was just whatever. They thought it was pretty, they liked the way it looked, they called it “sweat of the sun” and silver “tears of the moon,” but it wasn't really anything special just like Ikea isn't anything special to us right now. Sure, everybody likes some cool Ikea furniture, but it's not like it's a 100 year old hand-carved mahogany wood piece of furniture – it's just Ikea.

The Incas had a moneyless society and value was placed on labor instead of items – sort of like what a Communist society is supposed to be like. However, just like many communist societies have turned out, it often devolved into harsh central planning and forced labor.

So, here the Incas were, just chilling out, minding their own business with all that gold and silver, when Francisco Pizarro came across the Atlantic from Spain seeking fame, fortune, and you guessed it – gold. He made his way to Peru in 1524. The Inca thought Pizarro and his men were great. They called them “Children of The Sun”. The next thing the Incas know, these “Children of The Sun” were back with three ships filled with twenty-seven horses, 187 men, and weapons like guns and mechanical crossbows.

The Incas had never seen horses or guns or crossbows and were terrified, but also confused as to why on EARTH these random people would want something as ridiculously trivial as gold and silver? Not only that, but why did they want so much of it? Even after their army was annihilated and King Atahuallpa tried to buy his freedom with 13,420 pounds of 22

carat gold and 26,000 pounds of pure silver, he was still killed and yet the Spaniards still wanted more. The Incas did not understand this and one was recorded as saying, "Even if all the snow in the Andes turned into gold, still they would not be satisfied."

To the Incas, gold was nothing but decoration, but for Pizarro and his men, gold and silver were more than shiny, decorative metal, it could be made into money – a unit of account, a store of value, a rare and valuable precious metal that could be minted and exchanged for goods and services.

In order for money to function correctly, it not only has to be scarce, rare, and desirable, it also has to be available, affordable, durable, fungible, portable, and reliable. Gold, silver, and bronze met all of these requirements and that's why it was the ideal raw monetary material used for thousands of years until just recently. The earliest known coins date back to 600 BC and were found in modern day Turkey.

The ironic thing is, that Pizarro and his conquistadors found their famed El Dorado, which translates into "City of Gold" and in the process discovered a mountain of silver, in which they forced the local population into mining. They were bringing so much gold and silver into Spain, that it provided a huge monetary stimulus and turned into a globally accepted currency (the first one of its kind). Yet, they dug up so much silver that the metal itself dramatically declined in value – its purchasing power with respect to other goods plummeted into a "price revolution" that affected all of Europe from 1540 to 1640. The cost of food sky-rocketed, rapid inflation occurred over all sectors and the currency went down in value. This acted as a "resource curse" in Spain, demonstrating that the value of money is only worth what someone else is willing to give you for it, therefore the value of precious metals (or anything on the planet for that matter) is not absolute. By increasing the money supply, they didn't make society richer, they merely drove up prices, devalued the currency, and went broke.

**So let's recap –**

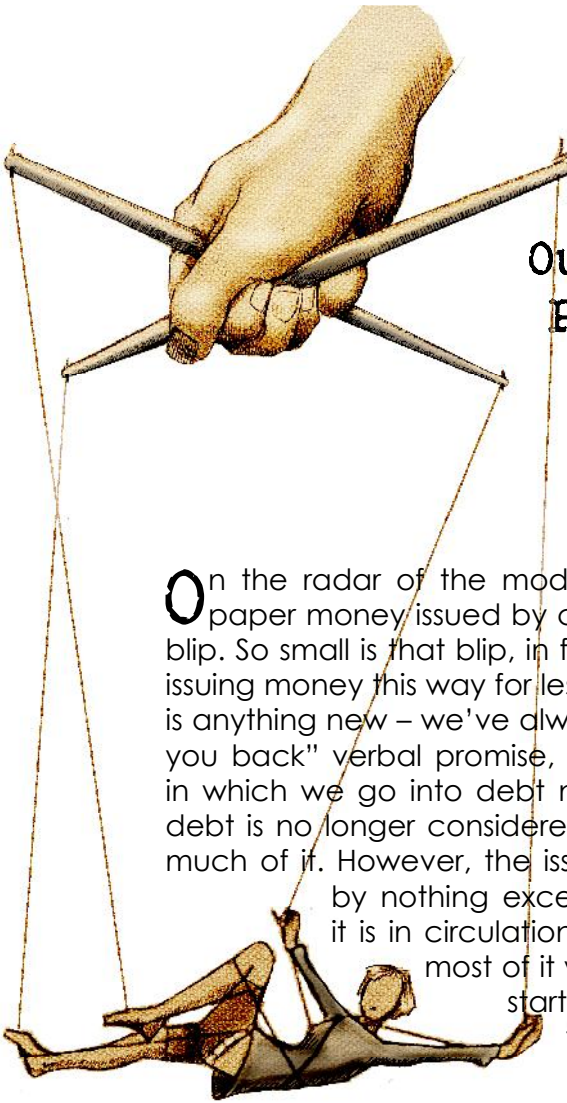
- Money is only worth what someone will give you for it
- What makes money worth something its scarcity, rarity, and desirability as well as whether or not it can be traded for tangible assets (food, water, shelter). For example, gold may be worth those things where I live, but it won't buy anything in ancient Peru.
- Money (general currency) can literally be anything of value, whether it be something you can hold in your hand, or a specialized service such as labor or knowledge.
- Don't expect anybody to care about your money during the zombie apocalypse.

But, we don't use precious metals anymore, we use paper currency, which also translates into digital currency, and it's backed by absolutely nothing (not gold, not silver, not wheat or barley). So, how did we get to this point?

## Chapter 2

### Our Current Monetary System Paper Currency, Centralized Banking, and Debt

---



On the radar of the modern human monetary system, our use of paper money issued by centralized banks is a tiny, teeny weeny blip. So small is that blip, in fact, that most of the world has only been issuing money this way for less than 100 years. This isn't to say that debt is anything new – we've always had that, from the world's first "I'll pay you back" verbal promise, there has been debt, although the ways in which we go into debt now have become very widespread and debt is no longer considered such a horrible thing, unless there's too much of it. However, the issuance of paper currency that is backed by nothing except people's faith in it and how much of it is in circulation is incredibly new, because up until 1972 most of it was backed by gold. However, in order to start our brief little journey of understanding into the developed world's current banking

---

structure, how paper currency works, and our endless cycle of debt, we first must understand where banks come from.

As has already been stated, debt is nothing new, and neither is the dreaded loan shark, which before the advent of banking, was the only kind of creditor out there, and the much feared loan shark began to run rampant in Northern Italy in the early thirteenth century, particularly in Pisa where merchants had to deal with all sorts of circulating coinage. If precious metals as currency had helped solve the problems brought about by the bartering system, the other problem was that there were so many different types of currency worth so many different amounts being offered up as payment for goods and services, it was only SLIGHTLY better than the previous system.

Not only that, but in this area the Roman numeral system was still being used, which created huge problems on a mathematical scale (but math is hard, and mostly boring, so we're not going to get too much into that). Suffice it to say, a genius mathematician by the name of Fibonacci decided to use the much more advanced system of mathematics borrowed from the Indian and Chinese, who had been more keen in these types of things throughout trade on the famed Silk Road.

Armed with an understanding of the Indian Method of mathematics, Fibonacci then combined Indian and Arab insights to completely change the way Europeans counted. Without him, we would not have the globally accepted Fibonacci sequence of numbers (0, 1, 1, 2, 3, 5, 8, 13, 21....) in which each successive number is the sum of the previous two – but again, we're not going to get too deep into that because, math is hard and stuff. Basically, if you can count and add  $2 + 2$  you can thank good ol' Fibonacci.

In Fibonacci's ground breaking book *Liber Abaci*, "the Book of Calculation" published in 1202, Europe now had the concept of present value (today's discounted value of a future revenue stream), Hindu-Arabic numerals instead of those pesky outdated Roman Numerals, the decimal system, fractions, the "Golden Mean", which is a repeating property found in the natural world, and generally just a bunch of stuff with numbers that made everything in areas of commerce easier – especially when it came to bookkeeping, currency conversions, and the calculation of interest.

With this new bookkeeping and numbers system came an orgy of money lending practices. In fact, the term "pound of flesh" was coined during this time in which the money lender must receive their pound of flesh as payment should their loan not be paid back with interest. The term comes from Shakespeare's "The Merchant of Venice" in which the villainously portrayed money lender Shylock demands the death of

one of his debtors due to his inability to fulfill the necessary financial obligations.

Today, the loan shark still exists and many people throughout the world rely on this primitive money lending practice in order to survive. You probably know about a half dozen classic Italian mob movies that center around the practice of illegal loan sharking, and the gruesome bullying on behalf of the mob in order to ensure their debts are paid back. Just as it was in Northern Italy over 800 years, so it is now., capicche?

It's easy to see how this type of money lending carried many weaknesses – the lenders ensured their loans would be paid back by using fear. However, even in those cases, many of them would find themselves without their loans paid back. In fact, in the early fourteenth century, there were three primary financiers that dominated the landscape – the Florentine houses of Bardi, Peruzzi, and Acciaiuoli. They were all three wiped out in the late 1300's because their clients defaulted on their loans, the two principal clients being King Edward III of England and King Robert of Naples. The weaknesses of money lending was becoming obvious, but as the Medici family would show, where money lending in the past had failed, the idea of the bank would succeed.

Without the Medici family, it's safe to say the Renaissance as we know it would not have taken place and flourished so widely as it did. The original Medici bank started out more like a stall on a street corner next to the Florentine wool market. Prior to the 1390's, the Medicis were more gangsters than bankers and were noted for their petty violence. Five of them were sentenced to death for capital crimes until Giovanni di Bicci de' Medici, who decided he would make his family legitimate through hard work, sober living, and a lot of careful calculation.

During this time, there were so many different currencies floating around it was confusing – some gold, some silver, some other base metals. Long-distance trade and tax payment was complicated to say the least. Medici was a money exchanger in that he converted currency using bills of exchange.

Let's say a business owner owed someone a sum of money that couldn't be paid in cash until a few months from now. The creditor could use a bill on the debtor as a means of payment in its own right or to obtain cash for it at a discount from the banker who is acting as a broker. Instead of charging interest, the Medicis instead profited from the transactions (they charged a small amount of money in order to handle the transactions).

In the long run, the reason the Medici banks stood the test of time was because, instead of other banks which were large structures that



could be brought to ruin from one large defaulting debtor, the Medici banks were made up of many partnerships, each based on regularly renegotiated contracts. Branch managers were not so much employees as they were junior partners who received a share of the profits. It was this kind of decentralization that helped make the Medici bank succeed.

The Italian Medici method of banking, which involved spreading their risks through making their banks large and diverse, effectively reducing vulnerability due to defaults, spread throughout the world to the North European nations such as the Dutch and English, as well as the Swedes. However, it was the Song Dynasty in China who first issued generally circulating paper currency and the Yuan Dynasty was the first to use notes as the predominant circulating currency.

Yet, in 1455, the Ming Dynasty ended the use of paper money and closed much of the Chinese trade in an effort to control inflation. It wasn't until the Bank of Amsterdam in 1609 that banking changed forever. This precursor to all modern central banking, was founded in Stockholm and answered to parliament. One of the roles of the Swedish central bank was lending money to the government, which is a trend and practice that would continue throughout the world.

However, it was the Bank of England that would become the model upon which most modern central banks have been based. It was devised by Charles Montagu in 1694 and got its start after loaning 1.2M to the government. In return, those who subscribed would be incorporated as The Governor and Company of the Bank of England, a title which carried with it long-term banking privileges including the issuing of notes.

When centralized banks such as The Bank of England first began, it was still developed under the international gold standard, which meant that paper currency could be exchanged for gold or silver and vice versa. The paper currency was similar to a promissory note, much like those old Mesopotamian clay tablets. Even better, is that it allowed people to deposit their money within the bank, and when they needed to pay someone, they could simply debit the account to their creditor (a system that many of us take for granted today as we can easily transfer money in between accounts using online resources and pay merchants using our debit cards).

Not everyone agreed with centralized banking though. In fact, one well-known country began a bloody revolution to get away from any kind of central bank. You know it as The United States of America.

In 1775 the American revolutionary war began. The American colonies were fed up with their English overlords and sought to detach from what they thought of as an oppressive monarchy. Although there were many

reasons for such a revolution – the likes of which had been festering within the colonies, forming a bubble ready to burst – one reason in particular that stands out as the prime cause is when King George III of England outlawed the interest-free independent currency that the colonies had been producing and using themselves.

Basically, the colonies were producing their own currency, which was decentralized and independent. They produced the money and used it for themselves, it was regulated on a local level publicly and not controlled by any one authoritative group. King George III wanted the colonies to borrow money from the Central Bank of England, at interest, which the colonies saw as debt enslavement. Benjamin Franklin, one of the United States' predominant founding fathers stated, "The refusal of King George to allow the colonies to operate an honest money system, which freed the ordinary man from clutches of the money manipulators, was probably the prime cause of the revolution."

Americans, were to say the least, very wary of any kind of centralized banking system because they didn't like the idea of money being controlled by a few people, nor the idea that the money would be lent to the American government to be paid back with interest using taxpayer money, which is essentially what a central bank is (we'll get more into that later).

In 1783 the American colonies won their independence from England, however the government would continue to battle with the concept of a Central Bank. Let's look at what essentially a central bank does – it is an institution that produces the currency of an entire nation or region. This Central Bank controls the interest rates and controls the money supply (inflation).

Remember – what makes money valuable is scarcity, desire, and the faith people have in it. If too much money goes into circulation then prices go up, and the value of that money goes down, just like what happened with Spain and the whole of Europe after Pizarro found his mountain of silver along with El Dorado. Left to its own devices, the worth money can fluctuate rapidly – such is the thought process of those who condone centralized banking. For example, if the U.S. experienced a massive influx of gold within its own borders (which it did on multiple occasions) then hyper inflation would hit.

What Central Banks seek to do is control a nation's money supply by lending a certain amount to the government on interest and controlling the amount of money that can be circulated at any given time. In effect, the thought process is that inflation will rise slowly over an even period of time rather than rapidly. The problem is, that many people distrusted an entire nation's money supply being given over to a small

group of dominant men, nonetheless ones with zero oversight, who could act behind closed doors, and lend money to the government. This meant that the entire United States government would be in debt to a private banking institution that it had no actual control over. This was the argument.

When the Central Bank supplies a government with money, it loans it to the government with interest. Then, through the use of increasing and decreasing the money supply, the Central Bank is able to regulate the value of the currency in circulation. This, in effect, can only produce long-term debt. For each dollar produced (let's just use the U.S. dollar for this example) it isn't actually a dollar – it's a dollar plus a percent of debt based on that dollar.

Essentially, the Central Bank has a monopoly on the production of currency for the entire country and they loan each dollar with an immediate debt attached to it. In addition, the money to pay off the debt attached to each loan must also come from the Central Bank yet again, which means the Central Bank must perpetually increase the money supply to temporarily cover the debt created. Since each new supply of money is loaned out at interest, it creates mounting debt, which essentially can't ever truly be paid back.

As counter-intuitive as this practice may seem, many people were pro-centralized banking in the United States once the United States government was set up. However, many presidents were completely against centralized banking and would strike them down whenever they threatened to be established, one of the largest anti-centralized banking presidents was Andrew Jackson who, coincidentally (or not) was president during the only time in U.S. history that the country was not in debt.

So, with all of this controversy, how did centralized banking finally take root in the United States? It took a series of panics. The first panic was the panic of 1907. Rumors began circulating about a prominent New York bank, the rumors were that the bank wasn't solvent and was bankrupt. This caused mass hysteria. The public feared losing their deposits and immediately began mass withdrawals. This caused the banks to call in their loans, which prompted their recipients to sell property, resulting in a spiral of bankruptcies, repossessions, and turmoil.

Throughout the years, many people have found evidence seemingly pointing toward J.P. Morgan – then a financial luminary – as the architect behind the panic of 1907. For example, Frederik Allen of Life Magazine wrote, "The Morgan interests took advantage to participate the panic [of 1907] guiding it shrewdly as it progressed." However, others see J.P. Morgan as an integral helper who aided in ending the panic.

Regardless, the panic of 1907 led to a hefty congressional investigation that was headed up by Senator Nelson Aldrich. This commission recommended that a central bank be implemented so that a panic on such a scale would never happen again. In 1910 a secret meeting was held at J.P. Morgan's estate on Jekyll Island off the coast of Georgia (truth is a little stranger than fiction in this case, it has been notoriously known as a very clandestine, cloak and dagger meeting ). It was during this meeting that the bill called the Federal Reserve Act was written, which was drafted by all bankers.

When Woodrow Wilson became president, the Federal Reserve Act was signed into law. Between 1914 and 1919 the Fed increased the money supply, which increased loans to small banks and the public. However, in 1920 the Fed called back a large percentage of these loans, resulting in the supporting banks calling in a large number of loans similar to what happened in 1907. Bank runs occurred, bankruptcy ran rampant, and collapse ensued. Over 5,400 competitive banks outside the Federal Reserve System ended up collapsing.

After the panic of 1920, the Federal Reserve once again increased the money supply, which stimulated the economy resulting in generous loans to the public and banks. At this time, a margin loan became very popular, which allowed investors to put down only 10% of a stock's price with the other 90% being loaned from the broker.

Basically, if you wanted to own a \$1,000 stock, you would only have to put \$100 down. This became incredibly popular and contributed to the roaring 1920's because it allowed pretty much everybody to start making money on the market. The only problem is that the loan could be called in at any time, which is a factor people overlooked, and which at the time seemed very unlikely – it was termed “A Margin Call”, which resulted in the selling of the purchased stock with the loan.

In 1929 the New York financiers who initially furnished the margin loans began calling them in. Naturally, this caused a huge sell off in the market for people who had to cover the margin loans. This, yet again, caused massive bank runs, which collapsed 16,000 U.S. Banks. After that, rival banks were able to swoop in and purchase the banks for cheap along with entire corporations (much like we saw happen with the sub-prime mortgage melt down, which we'll talk about later).

The Federal Reserve then made a decision that very likely caused the Great Depression – they contracted the supply of money rather than increase it. However, some economic historians such as American professor Barry Eichengreen blame the gold standard for prolonging the Great Depression by saying America's adherence to it is what prevented

the Federal Reserve from expanding the money supply in order to stimulate the economy, fund insolvent banks, and fund government deficits that could have caused expansion.

By this thought process, it was the gold standard that ultimately limited the Federal Reserve – or any other centralized banking system throughout the world (as Australia and banks throughout Europe were discovering) – from having the flexibility they needed to create money. It limited their ability to expand money supply and lower interest rates.

By law, the U.S. Federal reserve had to have 40% gold backing its demand notes. Therefore it could not expand the money supply beyond what was allowed by the reserves of gold held in the vaults. Federal Reserve Chairman Ben Bernanke and award-winning economist Milton Friedman have also written extensively about how the severity of the Great Depression was primarily due to the tightening of the monetary policy. In 1934 congress passed the Gold Reserve Act and ordered the Federal Reserve banks to turn over their gold supply to the U.S. Treasury, following the trend of many other countries around the world including Europe.

One of the primary reasons Congress enacted a joint resolution to nullify the right of creditors to demand payment in gold was due to the frightened public during the Great Depression, who were hoarding gold and had no faith in the economy, making the dollar increasingly worthless not only locally, but abroad. Because one of the best ways to fight off an economic downturn is to inflate the money supply, President Roosevelt was being coaxed into getting off the gold standard since it was impossible to inflate while on it. Roosevelt ordered on April 5<sup>th</sup>, 1933 that all gold coins and gold certificates of more than \$100 be turned in for other money.

Roosevelt ordered all people to deliver their gold coins, gold bullion, and gold certificates owned by them to the Federal Reserve for a set price of \$20.67 per ounce. In 1934 the government price of gold was increased to \$35 per ounce where it remained until 1971 when President Nixon announced it would no longer convert dollars to gold at a fixed value and thus the gold standard was completely abandoned. Then, in 1974, President Gerald Ford signed legislation that permitted Americans again to own gold bullion.

Many countries, including the United States, returned back to a certain type of gold standard after World War II, which was called a "gold exchange standard." This allowed for countries to fix their exchange rates in relation to the U.S. Dollar and central banks could exchange their dollar holdings into gold at an official exchange rate.

However, in just over 80 years of most of the world being under a centralized banking system, wild fluctuations have occurred, huge spikes in inflation have occurred, bubbles have formed and bubbles have burst, most of the world is tied up in crippling debt they will never truly get out of, and the only response to these things is to print more money, which will forever cause prices to continue rising and currency to continue losing it's value, which we'll talk more in depth about soon. This has caused many people to question central banking and desire something more tangible and predictable and large respected groups are actually calling for a return to the gold standard.

So, before moving on, let's look at a quick pros and cons list of a gold standard.

**Pros:**

- Long-Term price stability – a gold standard makes it incredibly difficult for governments or any kind of private organization (such as a central bank) to inflate prices through the circulation of paper currency. High levels of inflation are rare and hyperinflation is virtually impossible because the money supply is only able to grow at the rate in which the gold supply increases.
- Fostering of Economic Growth – When the United States returned to the gold standard from 1870 to 1912, the country experienced an increase in industrial production of 682%. However, it has increased only 159% from 1970 to 2012 where there was no gold standard. The United States had its greatest periods of economic advancement with a gold standard system.
- Fixed International Exchange Rates – For countries that adopt it, a fixed international exchange rate reduces uncertainty in trade. Strictly historically speaking, imbalances between price levels in different countries would be either partly or entirely offset by an automatic balance-of-payment adjustment usually called a price specie flow mechanism. By using gold to pay for imports, deflation and reduction in general price for goods and services occurs, making them more competitive.
- Zero Financial Repression – Alan Greenspan wrote in 1966 that, "Deficit spending is simply a scheme for the confiscation of wealth. Gold stands in the way of this insidious process. It stands as a protector of property rights. If one grasps this, one has no difficulty understanding the statist's antagonism toward the gold standard." John Maynard Keynes wrote, "By a continuing process of inflation, governments



can confiscate, secretly and unobserved, an important part of the wealth of their citizens." Therefore, Financial repression negatively affects economic growth.

### Cons:

- Unequal Distribution – Just like oil (a natural resource), gold is more advantageous in terms of cost and economic empowerment only for those countries that produce it.
- Constraints – "As an economy's productive capacity grows, then so should its money supply. Because a gold standard requires that money be backed in the metal, then the scarcity of the metal constrains the ability of the economy to produce more capital and grow."
- Less Options During Recessions – Mainstream economists, for the most part, think that economic recessions can be mitigated by increasing the money supply during economic downturns (which is something they wish could have been done to end the Great Depression sooner, and was the primary catalyst for going off of a gold standard). However, by following a gold standard, monetary policy could not be used to stabilize the economy in times of recession.
- High Short-Run Price Volatility – Even though the gold standard provides high long-term price stability, it has also been shown to have high short-term price volatility, which can lead to financial instability due to lenders and borrowers becoming uncertain about the value of debt.
- Production – Fluctuations in the amount of gold mined could cause inflation or deflation depending on if there is a sharp increase in gold or a sharp decrease.

All in all, at this point in time during our modern economy, it seems unlikely and frankly unhealthy to return to a pure or alternative gold standard, especially considering that the current amount of fiat floating currency in circulation FAR outweighs the amount of gold on the planet. However, at the same time it seems worrisome to allow a private centralized bank with low levels of congressional oversight or governmental control to solely determine how markets work, how much currency is circulated, and the rate of inflation, especially when these decisions are made behind closed doors because this limits the amount of security individuals have while strengthening the amount of security

the banks have.

Centralized banks have become a scary thing for a lot of people, especially when they really only care about the other gigantic too-big-to-fail banks with whom they do business. As Shah Gilani wrote in *Forbes* within an article entitled *It's Not Libor Stupid, Central Banks Are The Problem*, "Central banks are independent supra-national bodies who have been ceded monetary power by governments almost everywhere to benefit banks and bankers the world over, who are their only constituents, and for all intents and purposes, effectively 'own' legislators and governments."

This means that central banks and the mega banks which make up their constituency are beyond government control and are so large and unregulated, that they dare not be penalized when they commit outright fraud. They are given monopoly power over the national currency and they have considerable discretion in how to carry out their tasks without any kind of external accountability.

Take the sub-prime mortgage meltdown of 2008 in the United States, which caused one of the biggest world-wide financial collapses we have ever seen in our history of banking. The Federal Reserve provided over \$16 trillion in bailouts to banks and corporations in just a three year period, which surpassed both the national debt and the annual gross domestic product for the United States, thrusting tons of money into the economy all at once.

Here is a list of their bailouts:

- ▶ Citigroup: \$2.5 trillion (\$2,500,000,000,000)
- ▶ Morgan Stanley: \$2.04 trillion (\$2,040,000,000,000)
- ▶ Merrill Lynch: \$1.949 trillion (\$1,949,000,000,000)
- ▶ Bank of America: \$1.344 trillion (\$1,344,000,000,000)
- ▶ Barclays PLC (United Kingdom): \$868 billion (\$868,000,000,000)
- ▶ Bear Sterns: \$853 billion (\$853,000,000,000)
- ▶ Goldman Sachs: \$814 billion (\$814,000,000,000)
- ▶ Royal Bank of Scotland (UK): \$541 billion (\$541,000,000,000)

- ▶ JP Morgan Chase: \$391 billion (\$391,000,000,000)
- ▶ Deutsche Bank (Germany): \$354 billion (\$354,000,000,000)
- ▶ UBS (Switzerland): \$287 billion (\$287,000,000,000)
- ▶ Credit Suisse (Switzerland): \$262 billion (\$262,000,000,000)
- ▶ Lehman Brothers: \$183 billion (\$183,000,000,000)
- ▶ Bank of Scotland (United Kingdom): \$181 billion (\$181,000,000,000)
- ▶ BNP Paribas (France): \$175 billion (\$175,000,000,000)

The reason this is such a big deal for people now in the modern world, is that all of the people harmed for the irresponsible actions of the banks were not helped – their savings were destroyed in the meltdown, their homes were taken away, and their pensions and 401ks and so on were lost – why? Because of irresponsible lending on behalf of the banks.

Yet, it is those same exact banks that got bailed out, because they hold ownership stakes in the Federal Reserve so they have an incentive to bail each other out and not individuals with issues such as mortgage loans, car loans, and student loans.

What does this mean? It means that, essentially, central banks are in business for themselves and will do whatever it takes to survive, and in the process of that they have little to no government oversight, which means that a small group of people are able to determine the lives of millions. Not only that, but in order to deal with this meltdown the Fed printed more money in three years than it had in any other time in history, while simultaneously creating an enormous pool of money and tripling monetary reserves, which tells us that hyper-inflation is in the near future and that prices will be driven up and the dollar will lose its value even more.

The EU is bailing out banks left and right as well at the time of this writing, some of them with very heavy regulations such as with Cyprus bank. Let's look at that for a moment. Cyprus is the third largest island in the Mediterranean with a Greek-speaking population of about 1 million. This island has a very fragile economy and is part of the European Union. Its banks accumulated a lot of Greek debt and when Greece went through its financial crisis, banks in Cyprus lost a lot of money.

However, with Cyprus the European Union is doing something completely different with their bailout. They proposed to bail out the banks of Cyprus with \$13 billion in emergency assistance, but instead of implementing

new taxes or getting money from abroad, the government wants to raise \$7.5 billion through a one-time tax on Cypriot bank depositors.

What does this mean? It means that, if you had your money in a Cyprus bank right now, the government would simply take it away from you. If you had 100,000 Euros in the bank (or about \$130,000 USD) then 9.9 percent of that money would just disappear. Deposits that are less than that would have 6.75% of its money disappear.

So, if you were a Cypriot fisherman and you had managed to save up \$10,000 in life savings, you would have \$675 of that money taken away.

The reason this is so scary is that this type of bailout may spread in the future.

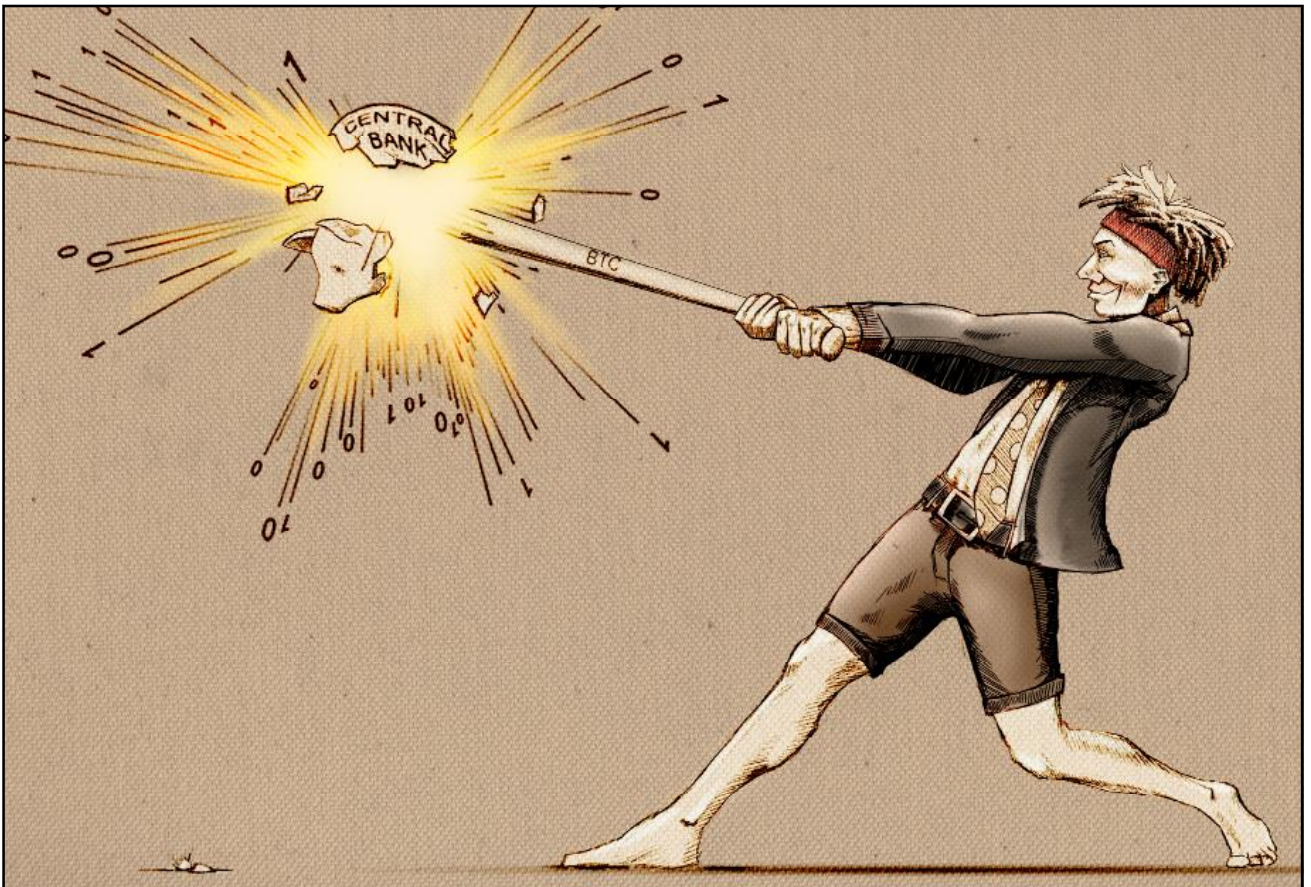
So, to recap, here are the problems we're faced with today as ordinary citizens:

- There are no tangible assets to back up our money supply (such as a gold standard)– it is printed out of thin air as floating fiat currency and a small group of people have full control over how much money is circulated at one time (central bank).
- That same floating fiat currency is printed by central banks who have full control over the government, serve their own interests, control interest rates and inflation, bail each other out when they cause massive financial melt downs, and are subject to virtually zero oversight or repercussions because they're "too big to fail."
- All of those problems involved with central banks and their mega bank constituents affects people terribly, because as we have seen through Cyprus and multiple other examples, as long as our money is in a bank, then it can be taken away from us right along with whatever savings we thought we could depend upon not being touched by government or central bank issues.
- Our money will NEVER go up in value, the entire system is designed for steady inflation over time, which means that our money can only decrease in value (unlike, a fixed gold/silver exchange rate).
- Countries like the United States are in so much debt that it is mathematically impossible to get out of it, not only that, but the very nature of a central bank lending money to governments means that they pay back their debts with taxpayer money, causing a vicious cycle that means no one is really debt free at any given time – ever.

**So, here's the BIG question....**

Is it possible to operate outside of this entire system? Is there a place to keep your money where government and central banks cannot touch it regardless of whatever kind of inflation or scams or bailouts are going on in the world? In addition to that, is there some kind of investment you can make that will go up in value, instead of down in value?

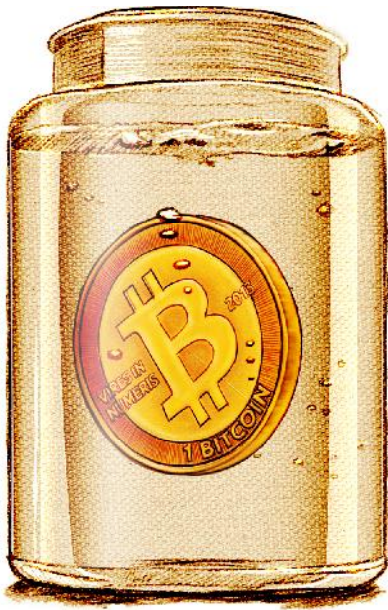
This, ladies and gentlemen, is where Bitcoin comes in...





# Bitcoin

## PART 2



### What is Bitcoin?

(Chapter 3)

### How Bitcoin is Changing The World

**I**n the last two chapters of this book we covered briefly, but still rather extensively, what money is, how it obtains its value, and the place of our modern banking system with all of its inherent pitfalls. Not many economists looking back in time will say that the gold standard was not a stabilizing way to handle currency. Unfortunately, as we've already explained, it would be impossible to go back on the gold standard today despite so many people calling for it. In just 40 years of being completely off the gold standard, bubbles have been created and have burst causing insane inflation and tons of money shot into the global supply, crashing and burning banks, causing bailouts, nearly collapsing entire economies,

---

and devaluing what we call money even more. The thing is, this is only going to get worse and there has been no solid idea on how to stabilize the world's income, until now and it's called cryptocurrency.

### What is Cryptocurrency?

First of all, it's important to understand that cryptocurrency is not something you can hold in your hand, which will inherently turn a lot of people off to it right away. So, let's get something out in the open right now – remember that those dollar bills (those pieces of paper) that you hold in your hand are not actually worth anything and in fact, they're not even real. The paper currency people are able to hold in their hands are just representations of worth, and the worth that is put on that floating fiat currency is based on nothing more than the faith people have in it paired with how much of it is in circulation.

Yes, paper money is printed, but it is still nothing more than digits and decimal points on a computer screen, as most of the money we use today is digitized. Furthermore, remember that the money you hold in your hand is not something that you truly own – the bank owns it because each dollar you have has been loaned to the government with interest, and in effect loaned to you on interest. So, in that sense, the idea of owning some form of tangible paper money is absurd – it's just a faith-based fiat floating currency controlled by a private organization with its own best interests at hand.

When we talk about cryptocurrency we're talking about a purely digitized currency. It is made using cryptography (we'll get more into that later) making it nearly impossible to counterfeit, and the way in which cryptocurrency came about is most interesting indeed, because it was and still is a rebellion to the current monetary system that many people see as corrupt, but necessary.

Earlier we talked about how the American Revolution really came about – the colonies had their own money supply that was regulated by the public – it was decentralized and it was a currency of the people that was not subject to inflationary moves by a central bank. It was when they attempted to force the colonies into accepting The Bank of England currency, that the final tipping point for the revolution occurred.



Cryptocurrency isn't much different in that sense. In the 1990's a movement known as "cyberpunk" emerged. Without going into too much detail, cyberpunk was a counter-culture phenomenon made up of hyper-intelligent tech-savvy young people who were taking advantage of the early World Wide Web. With this counter-culture came a lot of new ideas, one of which was known as cryptocurrency based off the modern mathematical theory and computer science practices of cryptography.

Cryptography is the practice of creating algorithms designed around computational hardness assumptions. Basically, it is blocks (think of a mountain made of rock) with information inside (think of the information as gold inside the mountain) and the cryptographic security surrounding it is what keeps the information secure (think about a huge wall surrounding the mountain with armed guards on top with rocket launchers). It is a way to encrypt information within secured blocks that are nearly impossible to break even by the most worthy of hacker adversaries.

The idea the cyberpunk movement had was incredibly innovative, and not much different from the idea the Americans had when they had set out to wage their revolution – what if we could create an alternative to traditional currency that required no central authority to administer it, that was easy to transfer, works across political boundaries, and belongs – once again – to the people on a public ledger?

The idea was so powerful, that it started gaining momentum as far back as 1995 when Seth Godin in his book "Presenting Digital Cash" wrote of Jon Matonis (a still popular contributor of alternative currencies for Forbes Magazine), "Matonis argues that what is about to happen in the world of money is nothing less than the birth of a new Knowledge Age industry: the development, issuance, and management of private currencies."

Andy Greenberg in his book, "This Machine Kills Secrets" also recounts the history of the 1990s cyberpunk movement, which paved the way for resources such as WikiLeaks and righteous hacker groups such as Anonymous who seek to expose corruption within government entities, financial institutions, and law enforcement. These early Internet crypto-anarchists saw a future world where widely available cryptography secured personal anonymity and privacy would be available to the point where it threatened the authority of the state. As Greenberg explains, their key insight is that anything that can be done cryptographically

can be done without government oversight.

They imagined online markets for information where buyers and sellers transacted anonymously using untraceable digital cash – anything from state secrets to private credit reports would be able to be purchased at the right price.

From that time onwards, some small attempts have been made on behalf of individual developers to create this cryptocurrency. However, all of those virtual currencies relied on third party intermediaries, such as bank or credit card companies to prevent “double spending” (more on this later). It wasn't until nearly 15 years later that somebody actually got it right and created the world's first usable cryptocurrency – Bitcoin – which relied on zero third party intermediaries and therefore became 100% decentralized.

### The Rise of Bitcoin

In June of 2011 Bitcoin soared in price value to a whopping \$32, which means a single Bitcoin could be exchanged for \$32 American dollars. It then fell promptly to \$2. In fact, this rise/fall trend continued until February 2013 when it peaked again at about \$30 and just kept rising. It rose so high, in fact, that it reached \$266 by April 10<sup>th</sup> 2013, and at the time of this writing has stabilized at around \$120. Right now, the total value of all Bitcoins hovers around \$1 billion.

Why is Bitcoin suddenly becoming so popular, and why is it suddenly worth so much now, when it wasn't worth barely anything before? Simply put, the reason is that it's becoming more legitimate. Remember in the first section of this book, we covered how people's faith in money largely determines its worth. The thing is, people are losing faith in banks and their own paper currency, while notable names in investment are beginning to buy up Bitcoins, journalists are talking more about Bitcoins, and more and more venues are accepting Bitcoins as payment, causing faith in the cryptocurrency to rise, thus increasing its value.

Let's look at some of the reasons Bitcoin is becoming more grounded as an acceptable currency:

### Legitimacy:

In May 2010 a US programmer swapped 10,000 Bitcoins that were then only worth about a cent each for two pizzas. That was the first ever Bitcoin purchase. As of April 2013 those pizzas would have cost him \$1.7 Million – if he had held onto those Bitcoins for three more years, he would have been an instant millionaire. In March 2013 a US citizen reportedly purchased a used Porsche Cayman using 300 Bitcoins. Later, we're going to talk more about why Bitcoins go up in value and why they're worth anything to begin with, but right now let's talk about the big names in finance whose investments into Bitcoin are causing more and more regular consumers and investors to have faith in the currency.

Charlie Shrem – a 23-year-old entrepreneur out of New York – has just opened up the first ever upscale lounges in NYC that take Bitcoins as payment. He is also one of the first Bitcoin millionaires. He created a startup called BitInSant, which makes it easy for people to quickly transfer Bitcoin funds, and is thus contributing to the amount of people who are beginning to use Bitcoin regularly while also making it easier for the average person to pay with Bitcoin just as simply as they would with their bank debit card.

Wordpress, OKCupid, and Reddit have begun accepting Bitcoins as a form of payment. At the time of this writing, it's been publicly noted that Ebay (and in effect PayPal, the online world's most preferred method of Payment) are looking into accepting Bitcoins, which could be the biggest legitimizer yet.

Offline, a gigantic variety of items are available to purchase using Bitcoins from cars to houses to Domino's pizzas to the hotel chain Howard Johnson. A Class Limousine is a black car service in New York that takes Bitcoin payments.

In early April 2013 Cameron and Tyler Winklevoss – the famous Facebook-claiming twins – purchased 1 percent of all Bitcoin. At the same time Andreessen Horowitz, one of Silicon Valley's most famous venture capital firms, announced its intention to invest in its first Bitcoin company – OpenCoin.

Investors in Silicon Valley such as Lightspeed, Greylock, Union Square Ventures, and more are all clamoring to invest in Bitcoin-related startups.

The more company's that invest in Bitcoin startups and the more retail locations both online and offline that start accepting Bitcoin as payment, and the easier Bitcoin becomes to exchange and use, the more legitimate the currency becomes and the more second-nature it becomes to use it.

## Decentralization

It's no coincidence that Bitcoin was created right on the heels of the sub-prime mortgage meltdown and all the bailouts and world economic problems that subsisted back in 2008. First of all, it's nearly impossible at this point to understand who exactly created Bitcoin, as it was made under a the pseudonym Satoshi Nakamoto, which could have been an individual or could have been a group of developers. Regardless, it was in response to the increasing distrust the public was beginning to have in traditional currency and the way in which people's lives and money were being treated by the banks.

Bitcoin is the world's first decentralized digital currency. It is tied to no country. It is not under the control of any central bank and it cannot be minted on plastic, paper, or metal. We touched earlier on the history of digital currency and how previous attempts could not be purely decentralized because they relied on credit card companies to prevent double spending. Let's look at this deeper.

If you loan your friend a \$20 bill, you will no longer have it. However, in the past, you couldn't have been sure of that with digital currency. When the cash is in a digital file it can easily be copied. If I email an attachment of a document to you, there is another copy right on my computer. The solution was to entrust an intermediary to keep a ledger of balances and deduct a transaction's amount from the payer's account, and add it to the payee.

The problem with this is that intermediaries are the choke-points where government can apply pressure. A great example of this would be when WikiLeaks released its State Department cables, and payment processors such as Visa and MasterCard gave into political pressure and refused to transmit donations to the group. Even PayPal froze accounts so the group couldn't access their funds. However, people could still donate Bitcoin.

What sets Bitcoin apart is it has found a way to solve this double spending

problem without using an intermediary – there is only ever the payer and the payee, which makes it literal digital cash. Bitcoin accomplishes this by a publicly distributed ledger of transactions across a peer-to-peer network. That means a record is kept on all transfers so that the same Bitcoin can't be spent by the same person twice. Because this ledger is distributed, there's no single central authority keeping it. Essentially, this makes Bitcoins TRUE digital cash just like dollar bills and euros – when you pay them to someone, you no longer have them.

The funny thing is that, while the American public is trying to pass bills to provide Congress with more oversight into the actions of the Federal Reserve (audit the Fed bills) Bitcoin's ledger is public and you always know what's happening with it. On the one hand, your traditional central bank does everything behind closed doors and effectively holds the entire future of our economy in their hands and under their discretion without accountability from any outside source, yet with Bitcoin this is impossible and it belongs to the people.

Because there is no third party regulating the ledger, there is no government, bank, or any one person or organization for that matter that can regulate it. That means, that if you transfer money into Bitcoins they can't be touched, nor can they be affected by whatever economic conditions are affecting your bank. They will, in truth, be completely off the radar and untraceable by government or banks. In effect, the money actually BELONGS to you again, and not the banks nor the government – it's 100% yours and no one else's.

Due to this decentralization, people all over the world who saw their savings destroyed in the economic downturn of 2008 and have seen the constant scandals coming out such as the Libor scandal – the worst banking scam in history, in which we saw small groups of people fixing interest rates across the board that affected nearly the entire developed world's money like it was nothing more than a game to them – have begun to invest in Bitcoins.

For example, someone who had money in a Cyprus bank and didn't like the idea of 10% of their earnings being taken out against their will during the EU bailout, could have taken that money and put it into Bitcoin where it was untouchable.

The idea of a currency that puts power back into the individual's hands, where they can actually own their money again and spend it or invest

it as they see fit, while being able to transfer it across countries without worrying about it is incredibly attractive. The less faith people have in centralization, the more faith they put into the first ever decentralized digital currency, which causes Bitcoin to become, yet again, more legitimate and trusted. This is what is making it increase in value.

### It's Like Gold, But Better

As we talked about in the first section of this book – gold isn't valuable because it's shiny, it's valuable because it's useful as a currency. There is no particular point in which we need to ask ourselves if Bitcoin money is valid or if someone can lie to us by providing a true or false answer. Bitcoin is valid locally – like gold – and it subdivides as easily as any number on a computer. Just as gold is intrinsically gold, so is Bitcoin.

Later we're going to talk about how Bitcoin is mined just like gold, but right now let's just draw some simple comparisons to how gold is mined, because it's essentially the same thing.

Gold grows naturally and it is naturally available throughout the world, it is also subject to demand. As demand for gold grows, the more people out there will want to mine for it. At the beginning, random miners used to be able to just show up at a stream and make a fortune panning for gold – it was the low hanging fruit of this precious metal, you just walked right up and picked one and didn't need a lot of money to get started, nor did you need any special tools.

However, as demand for gold grew, the surface gold was taken up as more and more prospective millionaires went to seek their fortune. At a certain point, the demand for gold grows so high that more comprehensive mines have to be opened, the likes of which can only be organized by major corporate and state backers who are able to put the amount of people and capital together to acquire gold at that scale. Complicated machinery is then used to mine for the gold, and new innovative techniques must be used in order to bore into the earth and mountains to find the deeper strains of gold. As demand grows, supply lessens, and it becomes more difficult to mine for the gold.

Bitcoin adopts a lot of these properties. When pressure for gold allows

new mines to be opened, thus increasing the supply, strong pressure for Bitcoin does the same. The difference, however, is that the supply doesn't change with Bitcoin, only the distribution.

So, in the case of Pizarro, which we discussed in the first section of this book, the fact that he opened his new mine in South America and started hauling all of that gold/silver back to Europe effectively caused inflation. But, with Bitcoin, opening a new mine in South America would be like reducing production of a mine in South Africa.

Bitcoin is better than gold in that gold doesn't have a good enough distribution process. It's just a commodity traded on electronic networks. People can lie about how much stuff they really have, and they do it all the time. There is no way to tell – sometimes they know they're lying with “naked shorts” sometimes they don't with “proven reserves” but the supply can always adapt to meet the demand – not with Bitcoin.

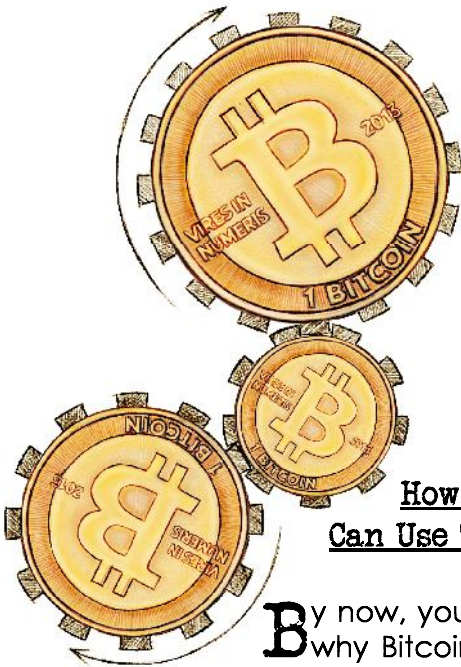
With Bitcoin everything is backed by cryptographic keys. One can actually prove they have access to a certain amount of it. You either are assigned messages linked to private keys or not. That's why the Winklevii twins said, “We have selected to put our money and faith in a mathematical framework that is free of politics and human error.”

Again, will get more into how Bitcoin works on a specific level (how new Bitcoins are created and mined and how many can ever be in distribution) later, but suffice it to say that they are like gold, only better.



# Chapter 4

## How Bitcoin Works



### How Bitcoins Are Created, and What You Can Use Them For.

**B**y now, you should have a fundamental understanding of why Bitcoin is valuable and why people are using them.

Now, the question is, how exactly do Bitcoins work? If they're purely based online, then how are they created and what makes them worth anything?

For most people who are used to traditional currency, the very idea of a digital currency can be very confusing because you can't hold something digital in your hands and you don't know where it comes from. In this chapter we're going to demonstrate exactly how Bitcoins are

---

created and what gives them their worth. We're also going to explore the various ways you can use Bitcoins in your everyday life by demonstrating how they can be used as a means to store money, exchange money, and invest your money before moving on in subsequent chapters on the specifics of how exactly to go about purchasing and trading Bitcoins.

## Bitcoin Creation

So far in this book we've talked a lot about gold and mining gold, now we're going to apply that knowledge to Bitcoin because the entire system of Bitcoin creation was based off the same model of mining.

Remember how gold mining works – over time it becomes more and more difficult to mine for gold. First, gold can be panned in a particular gold-producing area. This allows individuals with no startup money or even a crew to pick gold up right off the surface. As more and more people mine for gold this way, the surface gold begins disappearing, so more advanced techniques must take place in order to continue producing gold such as digging into the nearby mountain.

This means, that just one individual with a pickax isn't going to be able to do a very good job. So people with more capital and more equipment and a team of people come in to mine for gold and produce more of it. As time goes on, less and less gold is produced from the mountain and it takes more and more work to dig it out because gold is a non-renewable natural resource that takes thousands of years to create.

Now, let's apply that same principal to Bitcoin. Remember what we talked about with cryptographic technology? Essentially, the miner in this case is one individual with a computer. Back in 2009 when Bitcoin first started, an individual could download a particular software that worked at mining Bitcoins. The software chipped away at cryptographic blocks of information by attempting to solve mathematical problems. Once a mathematical problem was solved, the person who was mining was awarded with a Bitcoin.

A good way to understand this is, instead of going up and panning for gold, you were instead required to answer a riddle. If you answered the riddle correctly, you received a little bit of gold. However, as time goes on, the riddles get harder and harder to understand. After a while, you need a think tank of people who are working around the clock to solve these riddles so that they can get more gold. It's the same thing with

Bitcoin.

As time has gone on, the mathematical equations that must be solved in exchange for Bitcoins just keep getting more difficult. No longer can just one person with a consumer-grade laptop install a piece of software and expect their computer to mine Bitcoins. Now you have entire operations – teams of people with super computers and specialized software designed to run 24/7 solving complex mathematical problems for more Bitcoins. They're like giant mining rigs. In fact, Bitcoin mining operations often costs thousands upon thousands of dollars to set up and maintain every month.

At the time of this writing, every 10 minutes sees the creation of 25 new Bitcoins. However, this figure is cut in half every four years, which means after 2013 12.5 Bitcoins will be created every 10 minutes and so on, and the mathematical equations that must be solved in order to mine Bitcoins will become even more complex.

This will continue until the final Bitcoins are created in 2140 and only 21 Million Bitcoins will ever be in operation. This means that no centralized authority can inflate the supply and devalue the currency, and the currency will increase in value over time.

So, you see, Bitcoins are mined pretty much just like gold, except instead of using pickaxes and dynamite to mine, we're using computers and software to mine.

## What Can Bitcoin Be Used For?

### Trading (Buying and Selling)

One of the best and fastest ways to benefit from Bitcoin is through short term investment. Bitcoin prices fluctuate up and down just like stocks on the market do. It's easy for people to buy low and sell high for profit. You don't have to be some kind of financial wizard to do this, all it really takes is a discerning eye. Later we'll talk about Mt.Gox, but suffice it to say, simply keep your eye on the market. When the price of Bitcoins goes down a little – buy a few Bitcoins. Then, when they go up 10% or 20% or higher, sell them off for a profit. Many people like to do this

every couple of days to continuously profit from Bitcoin on a short-term time scale. You'll often see people buying \$1,000 worth of Bitcoins at the beginning of the week and selling them at the end of the week for \$1,700. It's a great way to make extra money on the side, or if you're really serious, you can even choose to do this full time.

### Long-Term Investment

Another great way to use Bitcoin is as a form of long term investment. Most economists and forecasters agree that Bitcoin is here to stay, and it's only getting more and more legitimate as time goes on and interest builds. That demonstrates great long-term value. You may want to buy up Bitcoins when they're low every couple of weeks or months and store them in your wallet in hopes of keeping them for a long time. Five to ten years from now, the 17 Bitcoins that you paid \$2,000 for could be worth \$20,000 or more. You can also mix buying/selling Bitcoins with long term investment by periodically selling off Bitcoins when the market is high, while keeping a store of Bitcoins for long term investment.

### Quick Money Exchange

You don't have to use Bitcoin as an investment tool in order to benefit from it. One of the great things about Bitcoin is its ability to allow users to quickly and easily send money to each other across borders. If you need to send someone \$1,500, for example, you could transfer that money into Bitcoins, send those coins to the appropriate wallet (we'll get into how exactly to do this a little later). You can also receive Bitcoins in the same manor. This is a way to use Bitcoin just as a quick tool, drop your money in, and take your money out.

### Buy Stuff!

As previously discussed, a growing number of online and offline venues are accepting Bitcoin now as a form of payment. Later we'll explore the various places where you can use your Bitcoins.

## Chapter 5



### Buying & Selling Bitcoin

#### How it's done

**P**urchasing Bitcoins is a relatively simple process, and if you have any experience in traditional banking, catching on to how to transfer traditional currency to Bitcoins and back again will be no problem. Basically, if you've ever written/deposited a check and even dabbled in online banking (checking your account balance online, transferring money from one account to another) then the process of purchasing, trading, sending, and receiving Bitcoins will be a snap for you.

But before purchasing Bitcoins, you need to know where and how they will be stored once you have them.

---

## The Bitcoin Wallet

Essentially all Bitcoins are stored in a Bitcoin wallet (not much different than your wallet or purse). This is where you will send Bitcoins from and where Bitcoins will stay once received. However, just like your physical wallet, it's important that you take measures to protect it because it can be stolen or lost. This is a reality for anyone in any situation, and Bitcoin is no different.

There are four types of Bitcoin wallets. You don't have to use just one type, and you can send money to and from each wallet as you see fit:

- **Paper Wallets**
- **Software Wallets**
- **Mobile Wallets**
- **Web Wallets**

Each type of Bitcoin wallet has advantages and disadvantages. If this seems a little confusing at first, a good way to think of it is all the ways you currently store money. No doubt you have a bank account, you also have physical cash in your wallet, you also have a mobile app for your bank in which you can check your balance and pay for things with. You may also have a PayPal account for online payments as well as a safe where you keep things like rare coins or sensitive information. You may also have savings accounts, multiple checking accounts, or safety deposit boxes.

All of these are various ways you store currency and other valuables – all of them have their weaknesses. For example, your online bank account can be hacked during an online purchase. If you have physical cash in your wallet, you can accidentally leave your wallet lying around, it could fall out of your pants, or someone could steal it from you. If your money is in a bank, the bank could experience problems like the ones in Cyprus did. If you have your valuables stored in a safe, the safe could be stolen or destroyed due to fire. Nothing is 100% secure, and neither is Bitcoin. However, by storing your currency across multiple channels, you help to ensure your eggs aren't kept all in one basket.

## Paper Wallets AKA "Cold Storage"

The Bitcoin paper wallet is the most secure form of Bitcoin storage because it allows you to store your coins independently of a computer or in another kind of offline storage media, which decreases the chances of your Bitcoins being stolen by hackers or computer viruses. Paper wallets are the equivalent of having your own personal safe with your gold stored inside – you can hide it and keep it forever. It's your own bank vault. The only way it will be destroyed is if you lose the safe, a natural disaster such as a house fire or a flood destroys the safe, or you leave the safe open so to speak allowing someone to just walk in and take what's inside. Just like a safe, people use paper wallets typically for long term savings of Bitcoins.

Here is how paper wallets are different from the other wallets we're going to talk about. Every time you want to send or receive Bitcoins or access a Bitcoin wallet with the other options we're going to talk about, you need a Bitcoin address, which is generated from a public key. Each public key also has a private key that unlocks the address. If someone is able to get access to this private key, they can get to the coins inside.

With a standard Bitcoin client – like the ones we're going to talk about later – your private keys are stored in a file called "wallet.dat." This is right on your computer. If the file isn't encrypted, then any virus or individual hacker can take your coins. However, if it is encrypted, then you will have to enter a password every time you make a transaction or want to access your wallet. Even though this is relatively safe, it is still vulnerable to keylogging, so it's not 100%.

The idea behind a paper wallet is, if the Internet never actually sees your private keys, there is no possible way any person could get access to them. In order to do this, the keys have to be created offline and printed out on paper where it can be stored offline in a secret place no one can find.

This can seem a little strange, especially since Bitcoins are digital currency – how on earth can you generate private keys for them without being online? It's actually really simple.





English | [Español](#) | [Français](#)

Open Source JavaScript Client-Side Bitcoin Wallet Generator

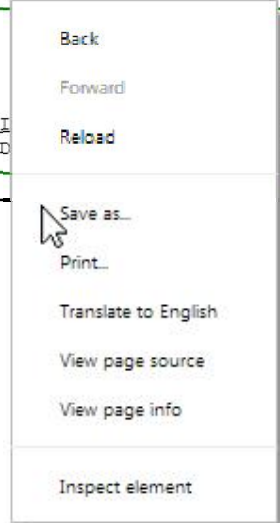
- Single Wallet
- Paper Wallet
- Bulk Wallet
- Brain Wallet
- Vanity Wallet
- Wallet Details

Generate New Address

Print

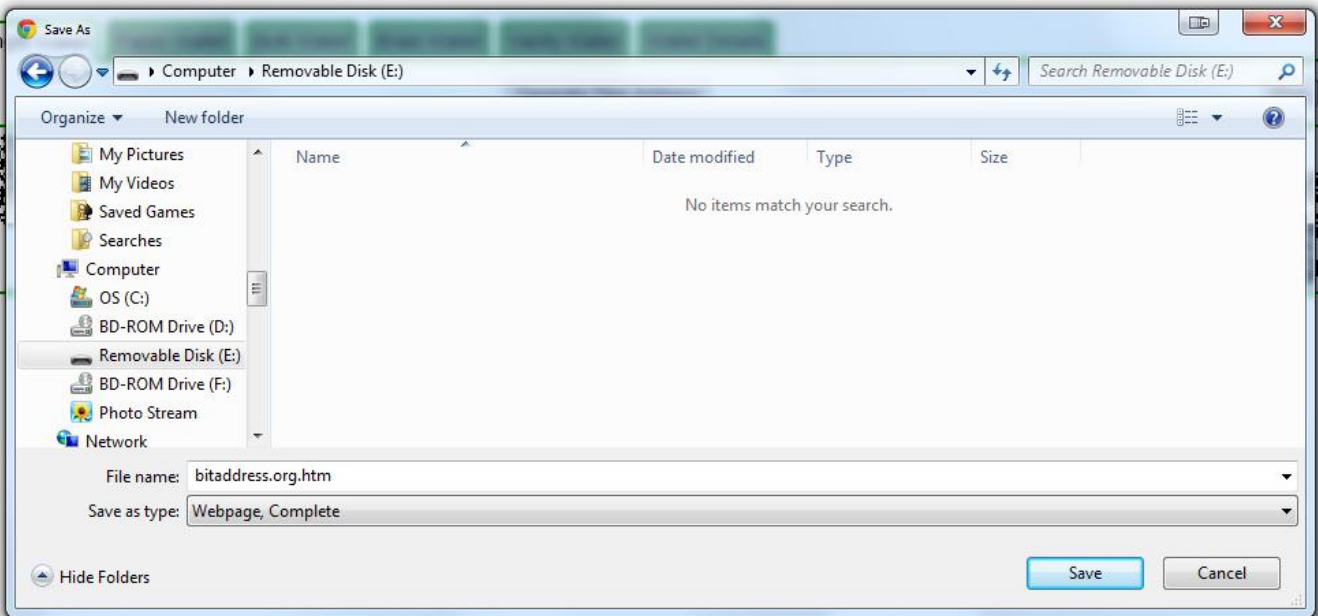
Bitcoin Address:  
1GqeeZW63XcZhr8NNNMaBfAm1RaihPwyrB

Private Key (Wallet I  
5Jwqz2Ug f4 fWwso fFREqNgqx F4NvqWugx z 9TD



### Go to **BitAddress.org**

Select "File" and "Save" on your browser, or just press the following keys at the same time: ctrl S. This saves the web page to your computer and since the webpage is javascript, even when the Internet is shut completely off, you will be able to use the website.



Plug in a USB Zip drive and save the web page to it.

Unplug the Zip drive and turn off the Internet.

Restart your computer with a “clean boot” by using a bootable CD such as Linux Live CD. This will ensure that your computer has no active spyware and that you are not connected to the Internet. This step is not completely necessary, and is simply an extra precaution should you decide to take it.

Once your computer is restarted, without turning your Internet back on, connect your USB Zip drive and double click the web page you saved. Even with the Internet off, it will come up on your browser.



Click the “Paper Wallet” tab, and then print out as many paper wallets as you want. It’s always good to have a variety of them, because later you can add any amount of Bitcoin you wish to each paper slip.

Now, the question you probably have, is how the heck do you put Bitcoins onto this piece of paper? Well, you will notice just by looking at the site that there is a “Bitcoin Address” that says “Load and Verify” with a scannable QR code and a “Private Key” that says “Spend” with a scannable QR code.

Later on in this chapter, we’re going to talk in depth about how to send

Bitcoins to your wallets (no matter where they are), but right now all you need to know is that the Bitcoin address you see there is what you will use in order to send money.

Now that your paper wallets are printed out, all you have to do is send money to the Bitcoin address printed on it, essentially loading up your wallet with money, and no one can ever hack it because the private key was never online and there is no trace of it. Every Bitcoin exchange such as Mt.Gox (again, we'll talk about that later) allows you to redeem paper wallets by typing in the private key code that's printed out.

Basically, if you send 100 BTC to your paper wallet, you can keep it there for as long as you want, and then transfer the BTC in that wallet online using the private key.

It's important to note that, if you misplace your paper wallet prints or accidentally throw them away or anything else, then the money stored on them will be gone forever (unless of course you have a photographic memory and can recall the addresses).

You can take this paper wallet and store it in a safety deposit box at your bank, put it in a safe, or just place it in a special drawer in your home to keep it safe. This is great for long-term storage and it will ensure no hacker or virus can touch your Bitcoins ever.

You can also do something similar to paper storage by taking screen shots of the addresses and storing them on a USB Zip drive. You could even encrypt the zip drive to where, if someone stole it, they would have to have a password in order to get into it. That's just another option.

There is another option as well. Blockchain.info has a hybrid paper wallet that allows you to store your Bitcoins offline and online, but also quickly transfer them back and forth. Here is their very detailed tutorial: <https://blockchain.info/wallet/paper-tutorial>

## Software Wallets

Software wallets are probably the most common and also most popular

way to store Bitcoins. These wallets are installed onto your computer and give you complete control. This means that you are charged with handling the security of your wallet. If you have a software wallet, then this means that if your computer crashes during a freak thunderstorm one night and all of your data is lost – so are all the Bitcoins stored on that computer. If you have hundreds or thousands of dollars worth of Bitcoins on your computer, and it crashes, then you'll never get them back. It's the same thing as withdrawing all your money from the bank, dropping it in the middle of the street, and burning it. That's not a very pleasant situation to be in.

On top of that, malware or spyware and other types of viruses that attack your computer while it's connected to the Internet can steal your Bitcoins and so can individual hackers. This is why you have to take extra steps to protect your software wallet, which includes the following:

*Encrypt your wallet so that it's safe from hackers and viruses* – this means that you will have to type in a password every single time you want to access your wallet or make a transaction. This will protect your wallet.dat file, which contains your private account keys, from being stolen by hackers and viruses. That's not to say that your wallet will be 100% indestructible because software such as keylogs can be used to crack your password codes (it's always a good idea to have large sums of Bitcoins put away in paper wallets, just like you wouldn't carry around thousands of dollars in your pocket wallet). Most software wallets will have helpful encryption options in place.

*Back your wallet up in case your computer crashes* – Most people these days know that they should back up their files in case of a crash, and your wallet should be no different. There are a variety of ways you can back your computer up. You can back your computer files up on external hard drives in your home. However, many people opt to back their computer up using online backup systems, which is still okay, but remember that these sources – because they're online – can also be hacked. The two sources that are the safest are backing your files up on a cloud-based system so that you can restore your wallet.dat file or by backing up your wallet.dat file using encrypted paper (this is probably the safest, since you can't hack paper, here is a post on how

To do that: <http://bitcoinplaza.blogspot.com/2013/04/how-to-backup-and-restore-bitcoin.html> )

There are a variety of software wallets out there for you to choose some, but here are the most recommended:

**Bitcoin-Qt:** This is the original Bitcoin client and it is the backbone of the entire Bitcoin network. It has the highest security, privacy, and stability of any software wallet. The only drawback is that it has fewer features and it takes up a lot of space and memory on your computer.

**Multibit:** This is the lightweight alternative to Bitcoin-Qt and it focuses on being fast and easy to use. It synchronizes with the Bitcoin network just like Bitcoin-Qt and can be up and running in just a few minutes. It also supports a variety of languages and is the perfect choice for people who are less technologically inclined.

**Armory:** Much like its name suggests, Armory is an advanced Bitcoin client. It actually runs on top of Bitcoin-Qt, but expands its features for power users. It also offers many backup and encryption features including cold-storage on offline computers.

**Electrum:** This software wallet is all about speed and simplicity. The fact that it doesn't use up a bunch of your computer's resources is also a huge plus. Electrum uses remote servers that handle most of the complicated parts of the Bitcoin system, allowing you to recover your wallet from a secret phrase.

### Mobile Wallets

Just like a mobile app for your checking account, mobile wallets are typically not standalone operations and are usually tied to web wallets, which we'll talk about in a second. However, there is one popular mobile wallet that does not need to be associated with any online service in order to work and it's called Bitcoin Wallet. At the time of this writing, it's only available for Android and BlackBerry OS. It's compatible with QR code scanning and NFC.

However, most mobile wallets are just added perks of what's called a web wallet in that the app itself accesses the web wallet and allows you to do the same things on your phone as you would on your computer's browser.

Bitcoin Wallet: This is for Android and Blackberry OS

Paytunia: This is another mobile web wallet and it is powered by Paymium, which works with Bitcoin-central to give you access to various Bitcoin exchanges directly from your mobile device. This option IS available for iPhone and, at the time of this writing, there is an Android version pending.

### Web Wallets

Web wallets are by far the most convenient type of wallet out there, but with this convenience comes a greater security risk. Mt.Gox (we'll talk in depth about this in a moment) handles 80% of all Bitcoin exchanges and has been hacked more than once, resulting in many stolen Bitcoins. Realistically, as Bitcoin grows, so must online security, and web wallets are struggling to keep up with exponential demand. This is why power Bitcoin users typically only use web wallets for small amounts of Bitcoin or to simply issue quick exchanges, opting to keep the bulk of their Bitcoins in paper and software wallets.

Because web wallets host your Bitcoins, it's also possible for them to lose your Bitcoins as a result of any incident on their side. At the time of this writing, there is no web wallet service that provides enough insurance to be used to store value like a bank. Although web wallets allow you to use Bitcoin anywhere with less effort to protect your wallet, choosing one with care is very important.

The good news is that web wallets will most likely just keep getting more and more secure. Remember, Bitcoin is still in its infancy and so are the wallets in which we keep Bitcoins. As time goes on they will continue to get better and better.

Blockchain.info: Blockchain is an incredibly user-friendly wallet that acts hybrid by storing an encrypted version of your wallet online. However, the decryption happens in your browser, so it's important to keep your browser extensions and email backups up to date with what's recommended.

BIPS: This is a web wallet service courtesy of WalletBit. It allows you to



buy and sell Bitcoins with ease. It also offers cold storage options (paper wallet), wallet import, and a variety of simple merchant tools and features.

Coinbase: This particular wallet has been attracting a lot of big time investors as of late. It's by far the easiest to use and also provides users with an Android web wallet app and merchant tools. The reason it's so easy to use is because it integrates seamlessly with US bank accounts, so it's easy for users to buy and sell bitcoins by linking directly to their bank account.

Mt.Gox: This isn't officially a wallet, but many people use it as such. Mt.Gox is the Internet's biggest and most well known Bitcoin exchange. It has a variety of merchant tools as well. In addition to allowing you to buy, trade, and sell Bitcoins, you also have a web wallet and a corresponding mobile app.

How you store your Bitcoins is really up to how you intend to use them. If you're looking to invest long-term with Bitcoin, the best option would be to store the bulk of your Bitcoins in cold storage (paper wallets). If you're looking to buy low and sell high with Bitcoin for continuous short term investing, then a software wallet will do nicely for you. If you're looking for a quick money exchange, then a web wallet will and mobile wallet will be all you need. However, you can do all three of these things – allocate a certain amount of Bitcoins to your paper wallet for long term investment while buying/selling BTC on the market from your software wallet and doing quick exchanges through web wallets.

### Transferring Bitcoins between Wallets

Each wallet you have (whether it be a software wallet, mobile wallet, or paper wallet) has a Bitcoin address for loading BTC onto. In your MtGox account, click "Trade" and then "Funding Options" then click the "Withdraw Funds" tab and fill out the amount of BTC you want to transfer along with the correct Bitcoin address. Make sure that this address is correct, because all Bitcoin transfers are final and permanent. Regardless of the type of Bitcoin exchange you're using, whether it be MtGox or something else, you will be able to transfer BTC into your wallet by using the correct Bitcoin address.



## Buying Bitcoins

Now that you know where and how to store your Bitcoins, it's time to finally get around to buying some! I hope you're excited, because you're finally about to get your hands dirty and contribute to the Bitcoin economy – the first currency of its kind in the history of the world. It's pretty epic when you think about it on those terms, isn't it?

There are a few ways in which you can purchase Bitcoins:

**Over the counter** – Purchasing Bitcoins over the counter is typically done in cash (or money order) at a designated location. There are many locations you can go to in your neighborhood in order to deposit cash and have it converted to Bitcoin such as CVS and Wal-Mart to name a couple. Cash is taken to these locations along with the necessary information that needs to be filled out. The cash is then converted to however many Bitcoins it's worth (let's say, for this example, \$150 converts into 1.1 BTC) and is sent to a Bitcoin exchange (such as Mt.Gox or VirWox) or an individual Bitcoin wallet address (such as a software wallet, web wallet, or paper wallet). This is similar to depositing cash or a check at the bank by filling out a deposit slip. This is very fast, and your Bitcoins will show up in your wallet within about 30 minutes of your deposit.

**Online** - There are also many online vendors that privately sell Bitcoins for a small commission based fee and good old Google is the best way to find these. However these private online vendors still seem to be restricted to physical locations which means that in many places around the world it is still difficult to buy Bitcoins despite the Internet. The first Bitcoin I purchased was from [www.spendbitcoins.com](http://www.spendbitcoins.com) which is an Australian only private vendor, what a splendid day that was.

Buying Bitcoins through Paypal is rare because of the anonymous nature of Bitcoin transactions. You could easily claim not to have received your Bitcoins after you've paid for them using Paypal which would create a dispute on Paypal who tend to side with the buyer. This has resulted in vendors avoiding the use of Paypal completely.

**Direct Bank Transfer** – This is one of the simpler ways to buy Bitcoins and you don't have to leave your house in order to do it. If you've ever used PayPal, you have a solid understanding of how this might work. Simply link your current checking account up with the Bitcoin purchasing

service, and you're done! After that it's all up to how many Bitcoins you want to purchase.

**The Exchanges** - Then there are the Exchanges. They are the most popular way and the best way to buy Bitcoins...

### Bitcoin Exchanges:

At the time of this writing, Mt.Gox is the most popular Bitcoin exchange on the Internet and handles about 80% of all Bitcoin exchanges. This poses a significant problem to the entire Bitcoin economy. MtGox recently claimed to have suffered DoS (denial of service) attack, one of the largest I've ever heard of. This means that hackers overwhelmed their servers which significantly slowed down their services and disrupted the trading platform. It was an isolated attack but because MtGox controls so much of the Bitcoin market the entire economy was seriously affected.

All our eggs are in the MtGox basket, so to speak, and it's not good. Their monopoly affects buyer confidence massively and slows the growth of the Bitcoin economy substantially. Therefore I want to encourage you to use alternative exchanges like VirWox and Bitstamp.

To distribute the market across many exchanges would be beneficial to the entire Bitcoin economy including MtGox. It is better to have a 20% market share of a multi-Billion dollar industry than a 80% share of a billion dollar industry.

Below is a six month representation of the Bitcoin Price from bitcoinity.com. As you can see at the time of the attack the Bitcoin price was undergoing exponential increase reaching an apex of \$260 before it

bitcoinity.org/markets  
Hosting sponsored by Predict Coins

USD GBP EUR AUD CAD GBP RUB more  
mtgox bitstamp btxc sample



crashed. Over time however you can see that the Bitcoin price has undergone a steady increase. After the market crashed down from \$260 it has continued to grow along a steady trajectory represented by the blue line on the graph. We can therefore say that the "crash" was simply an inevitable market correction. However, it did coincide with, or was facilitated by the DoS attack on MtGox and caused widespread panic which could've been diluted if not for the MtGox monopoly.

The Bitcoin economy is young and extreme market fluctuations are to be expected but as the economy grows so these fluctuations become much less severe and far more predictable. Up to now though, Bitcoin has seen its fair share of volatility, doubt and criticism but it has survived and keeps on growing every single day.

### Signing up with an exchange:

Signing up with the various exchanges are all relatively similar. I still want to encourage you to use alternative exchanges if you can, depending on your location. But MtGox is still most accessible globally. So in the interest of widespread relevance I am still going to use MtGox as an example and go through it step by step. But like I said they are all very similar.

### **Mt.Gox (mtgox.com)**

Last price: \$129.37000 High: \$135.47000 Low: \$124.00000 Volume: 47419 BTC Weighted Avg: \$1. USD

**MT.GOX**

Trade with confidence on the world's largest Bitcoin exchange!

Mt.Gox is the world's most established Bitcoin exchange. You can quickly and securely trade bitcoins with other people around the world with your local currency!

[SIGN UP NOW](#)

Username Password [Login](#)  
or [Sign up](#)

HELP

**Step 1) Sign Up:** On the front page on mtgox.com you'll see a "Sign up now" option. Click it and choose a username and password. Make sure your password is long and strong – this means it should include lowercase

The screenshot shows a registration form with the following fields and options:

- Username:** A text input field containing "IdiotsGuideToBitcoin".
- Password:** A password input field with a strength indicator showing a full green bar and the word "Strong".
- Confirm Password:** A password input field for confirmation.
- Email:** A text input field with an email icon and a partial "@" symbol.
- Currency:** A dropdown menu set to "USD".
- Agreement:** A checked checkbox with the text "I have read, understood and agree to the terms of service".
- Submit:** A large green button labeled "SUBMIT".

and capital letters along with exclamation marks and numbers. It should not spell anything nor should it be something you use on any other account. Make sure you write this down and keep it for your records.

**Step 2) Activate Registration:** An email will be sent to the address you provided. In that email will be a confirmation code. Simply copy the confirmation code and post it into the "Confirmation Code" field on the

In order to enable your account, you need to enter your validation code on the Mt.Gox website.

Your confirmation code: **DKD9DE6X3YGYKN69**

Alternatively you can click on or copy it into your browser via this url:

<https://mtgox.com/signup/validate?ID=a199659e-73bf-4fbd-a94d-6fab989195d1&Code=DKD9DE6X3Y>

CREATE AN ACCOUNT

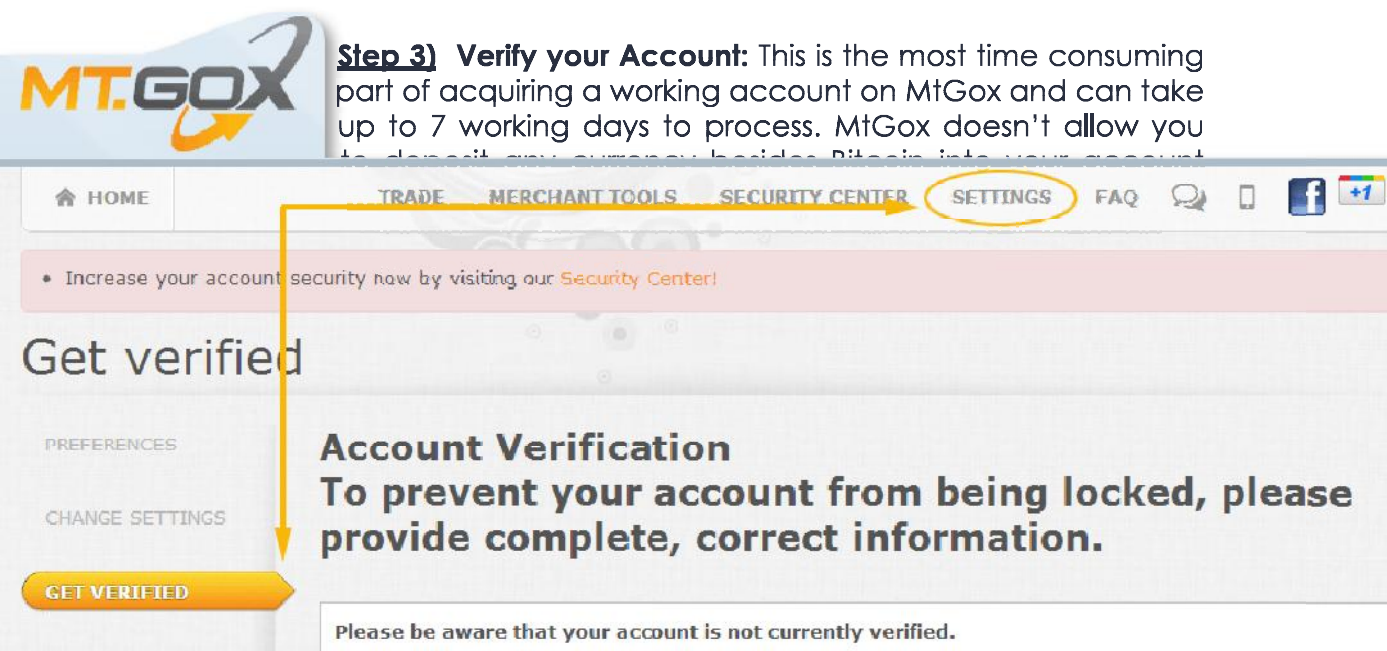
EMAIL SENT

**Thank you, your account is now activated**

Your account is now activated, you can start trading with Mt.Gox.

ACCOUNT ACTIVATED

mtgox website.



**Step 3) Verify your Account:** This is the most time consuming part of acquiring a working account on MtGox and can take up to 7 working days to process. MtGox doesn't allow you to deposit any currency besides Bitcoin into your account.

• Increase your account security now by visiting our [Security Center!](#)

## Get verified

PREFERENCES  
CHANGE SETTINGS

**Account Verification**  
To prevent your account from being locked, please provide complete, correct information.

**GET VERIFIED**

Please be aware that your account is not currently verified.

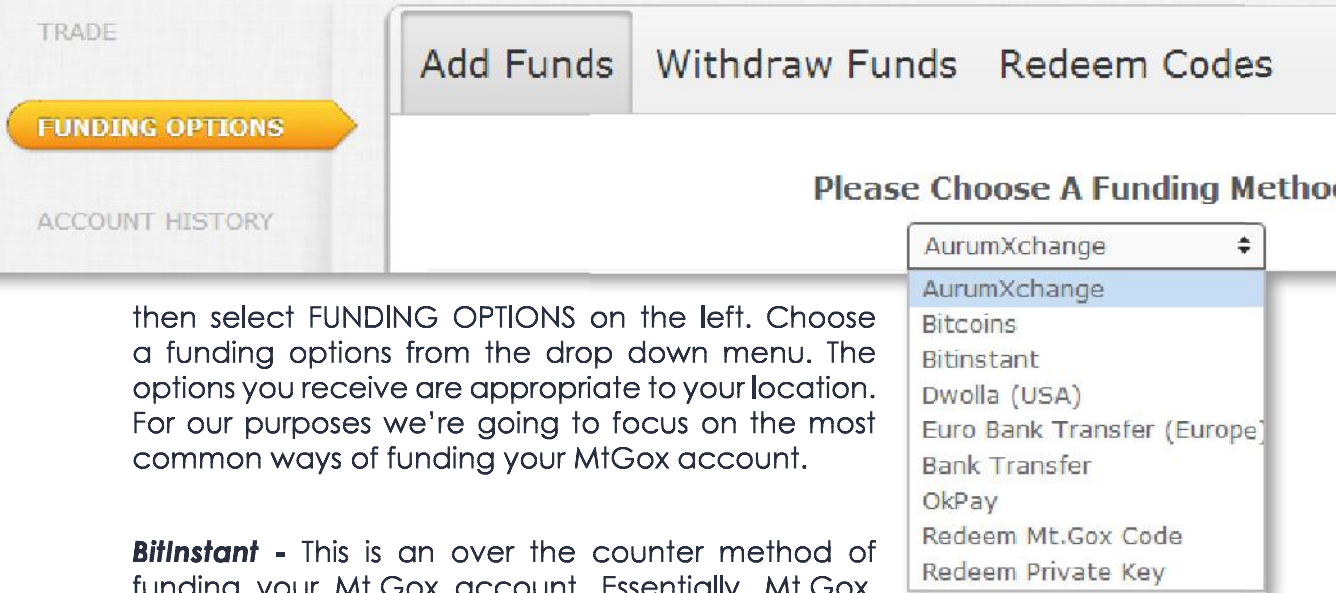
Once your account is activated go to the settings tab on the main menu You will be asked to upload:

- **VALID Photo Identification.** This has to be an official document like a passport, driver's license or Identity card.
- **Proof of Residence.** This has to be one of the following, Monthly Utility Bill, Internet Bill, Cellphone Bill, Tax return document, Residency Certificate, Medical Insurance Bill. The document that you submit has to be in your name and has to have been issued within the past 6 months.

Then you wait. A few days later you'll get an email that confirms your verified status and that's it. The hard part is over...

**Step 4) Fund Your Account:** You will now be able to select a method for funding your MtGox account. From the main menu select TRADE,





then select FUNDING OPTIONS on the left. Choose a funding options from the drop down menu. The options you receive are appropriate to your location. For our purposes we're going to focus on the most common ways of funding your MtGox account.

**BitInstant** - This is an over the counter method of funding your Mt.Gox account. Essentially, Mt.Gox, when you fund it, is a web wallet. BitInstant is a third party tool that you can use to fund your Mt.Gox web wallet and your software wallet and your paper wallet. It's a great tool. It's actually the fastest way to get your funds into your wallet, and often takes under an hour whereas the other methods we'll talk about can take 1 to 3 business days on average.

You can't use BitInstant through the Mt.Gox site. The best thing to do is open up a new tab on your browser and go to BitInstant.com. Once you get there the process is fairly straight forward.

Select a source to pay from. You will most likely be able to find a place right there that you recognize such as CVS or WalMart

Select a source you want to pay to (in this case it would be MtGox).

Fill in the necessary information below. The first thing you're going to see is the MtGox account number. In order to find this switch back to your MtGox account and look at the top of the page. You will see "Account number." Copy this and then past it into the correct field on the BitInstant website.

Decide how much you want to pay. Now, this depends on how many Bitcoins you want to purchase. You can start as large or small as you want. Keep in mind that you do not have to purchase an entire Bitcoin.

You can purchase what is called a Satoshi, which is a fraction of a Bitcoin. In order to find out what amount of money you need in order to purchase Bitcoins and Satoshis go back to your MtGox account and click "Trade" on the top left hand navigation on the "Buy & Sell" page. There you will see a converter. The best way to start is to enter in the amount of money you want to fund your account with on the far right. Let's say, in this case, \$50. Once you enter that in, the converter will automatically do the math for you. According to the current price of Bitcoins under that currency, the far left field will display how many BTC that allows you to buy. Anything after the decimal point is a Satoshi, anything before the decimal point is a full Bitcoin. Now that you know how much your currency will purchase in Bitcoins/Satoshi you're all set.

Go back to BitInstant and fill out the rest of the information – email, first and last name, date of birth, and so on.

After you fill this out you will be given a deposit slip (not much different than a deposit slip for putting money into your bank account). Print this deposit slip out and take it to the location you allocated. They will tell you what to do from there. Make sure that you have the correct amount of cash on hand.

Once you have deposited your cash you will be sent an email notifying you that the transfer was successful. After about an hour the funds will appear in your MtGox account.

**Bitcoins** - To fund your account with Bitcoins you have saved in another



The screenshot shows the 'Add Funds' section of the MtGox interface. At the top, there are three tabs: 'Add Funds', 'Withdraw Funds', and 'Redeem Codes'. Below the tabs, the text 'Please Choose A Funding Method:' is displayed. A dropdown menu is open, showing 'Bitcoins' as the selected option. Below the dropdown, an information icon (a lowercase 'i' in a circle) is followed by the text: 'To add bitcoins, send to this address (Please be advised that your bitcoin address will change every time that there is a transaction, but old addresses are still USABLE.):'. The Bitcoin address '1Bnk42qTRHi7MaNzNhBQjsg6ndv2aDNiYp' is highlighted with a yellow box. Below the address is a QR code. An arrow points from the text 'your wallet address' to the QR code.



location simply select Bitcoins from the drop down menu. You will be presented with a wallet address as well a QR code. Use this address whenever you want to add Bitcoins to your account. You can either save this address and use the it every time you wish to fund your account. Alternatively you can generate a new one every time. Both options are viable it just depends on the situation. Saving the address in your software wallet's address book is useful to save time.

**Dwolla** - Dwolla is only for US residents, but it's a fantastic and easy-to-use way to fund your MtGox account (and other Bitcoin exchange sites that we will talk about). Dwolla takes a couple of days to setup, but it's not much different than PayPal. First you have to go to Dwolla.com and create an account and link it to your current bank checking account. It takes about 3 days for an ACH deposit to go through that you need to confirm. Then, you can transfer funds from your bank checking account into your Dwolla account. Once that is in place, go back to MtGox and follow the instructions for funding.

**Bank Transfer** - If you've ever sent a wire transfer, you will know exactly what to do in this situation. Simply use the wire information provided. Go to your nearest bank branch and fill out the same information in order to wire money to your MtGox account. Again, during all of these examples, ensure that you know how many BTC your money is actually going to buy.

**Redeem Private Key (Paper Wallet)** - In order to redeem Bitcoins located in your paper wallet (cold storage) all you need to do is select "Redeem Private Key" from the drop-down funding options and type that key into the appropriate field. Easy as.

**Step 5) Buy Bitcoins** - Now that your MtGox account has been funded with cash, you will be able to purchase BTC. Log into your MtGox account and click on "Trade." You will see how much money is in your account. If you tick the 'market order' box you will be able to buy Bitcoins at their current rates. You can also set your own buy and sell prices but these orders are only executed once the market hits your desired price. Simple. That's it. You're trading.

Now that you have MtGox sorted I just want to reiterate that they are not the only exchange and that it is in all our interests to distribute the market share across multiple exchanges in order to strengthen and grow it.

The alternatives include the following:

- **VirWox (exchange)**
- **Bitstamp (exchange)**
- **Blockchain.info**
- **Local Bitcoins (over the counter)**
- **CoinBase (link your bank account)**

It's also important to note that, by using services such as Local Bitcoins, BitInstant, and Coinbase, you can fund your software wallet or paper wallet directly without going through an exchange.

### Selling Bitcoins

Whatever your level of participation in Bitcoin it is important to understand how to sell Bitcoins and quickly turn those ones and zeros back into dollars and cents when the need arises. This is important to know to maximize profit as well as avoid losses.

Luckily it's pretty easy to turn Bitcoins into Dollars without much delay. However, depending on your status with your exchange platform, you might have to wait a few days to gain access to those dollars but the important thing is that when the time comes, you can easily sell your Bitcoins for cash.

The quickest way to sell Bitcoins is on the exchanges. So if you don't have an account with one of them you simply have to create one. For that all you need is a name and an email address. The good thing about selling Bitcoins on the exchanges is that your account doesn't need to be verified to deposit Bitcoins into your account for you can sell them.

Creating an account with an exchange is covered on pages 49 and

50 of this Guide. Just follow step one and two. You'll then have to fund your account with Bitcoins which is covered on the bottom of page 53.

Once your account is credited with your Bitcoins all need to do is sell them. Create an ask (sell) order on the 'TRADE' page and be sure to accept the current market price if you want to sell your Bitcoins quickly. You can, of course, set your own price but then whether or not your Bitcoins sell or how long it takes depends on the market trajectory and depth.

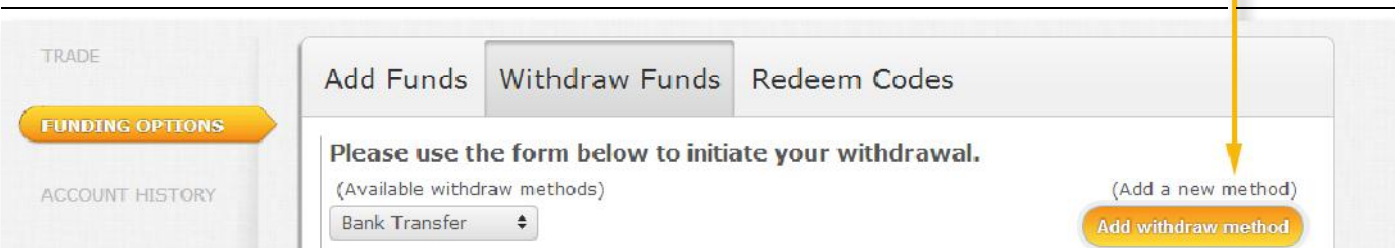
As soon as your Bitcoins sell your exchange account will be visibly and immediately credited with dollars (or whatever currency you've chosen). If you want to deposit the money into your local Bank account it is important that you make sure that you are trading your Bitcoins for your local currency. This is to avoid the costs and fluctuations involved when exchanging foreign currencies.

That's the easy part. The trouble is that on most exchanges you cannot withdraw fiat currencies without verifying your account, this is true for MtGox also. This means that if your account is not verified you will have your dollars but you will not have access to them.

At this point you have two options, both of which involve some length of time:

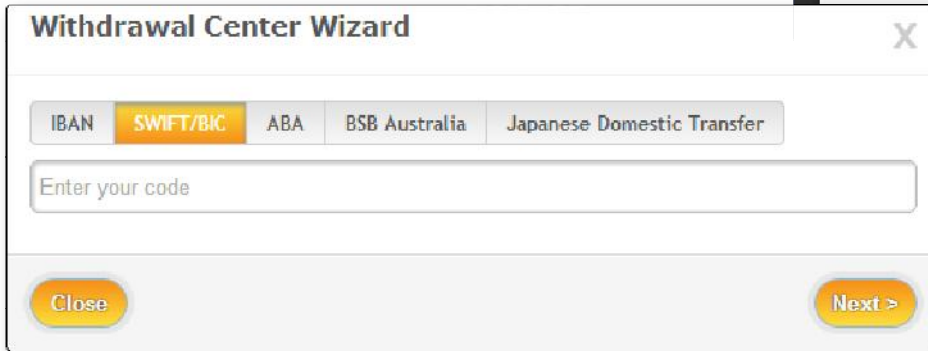
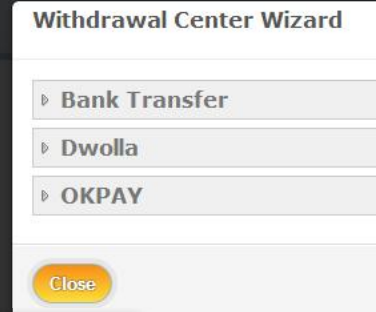
Your first option, which is only really viable if you are just avoiding a loss during a market price fall, is to just leave your dollars in your account and use them later to buy Bitcoins again when the market picks up. These can then be withdrawn without account verification.

Your second option is to verify your account (Step 3 on page 51). This will take a few working days but no longer than a week assuming the documentation you submit is correct and accepted.



Once your account is verified you will be able to withdraw fiat currencies. To do this, using MtGox as an example, you will have to create a withdrawal method.

Select TRADE > FUNDING OPTIONS > Add withdraw method.



You are then presented with three options: Bank Transfer, Dwolla and OKPAY. At the time of this writing Dwolla is indefinitely unavailable so we'll focus on the other two options.

**Bank Transfer** - Select the appropriate option. These options vary

**Withdrawal Center Wizard**
X

<b>Label:</b>	<input type="text" value="CITIBANK N.A."/>
	<input type="text" value="International"/>
<b>Transfer Type:</b>	International transfers include a ¥2000 fee, along with any intermediate bank fees.
<b>Your name:</b>	<input type="text" value="Your name"/>
<b>Bank Name:</b>	<b>CITIBANK N.A. (CITIUS33)</b>
<b>Your Account Number:</b>	<input type="text" value="Bank account number"/>
<b>Your Address:</b>	<input type="text" value="Your address"/>
<b>City:</b>	<input type="text" value="Your city"/>
<b>Postal Code:</b>	<input type="text" value="Your postal code"/>
<b>Region / State:</b>	<input type="text" value="Your region"/>
<b>Country:</b>	<input type="text" value="United States"/>
<b>Intermediate Bank (Optional):</b>	<input type="text" value="Intermediate bank swift code"/>

Close
Next >

depending on the physical address you entered when verifying your account. However international options like IBAN(international bank account number) and SWIFT/BIC are always available. Enter the appropriate code and hit Next>. In our example we are entering the Citibank USA swift code which is CITIUS33. You are then presented with

**Please use the form below to initiate your withdrawal.**

(Available withdraw methods)

(Add a new method)

A screenshot of a web form's dropdown menu. The menu is titled '(Available withdraw methods)'. It contains four options: 'Bitcoins', 'Bitcoin Foundation', 'Bank Transfer', and 'CITIBANK N.A.'. A yellow arrow points to 'CITIBANK N.A.'. To the right of the dropdown is a button labeled 'Add withdraw method'.

the form below.

Once you've completed the form you are asked to confirm the details you've entered. When you click Next it says "Beneficiary data saved" after which you will have to wait a short validation period usually no longer than a day or two. After which it will become available in the withdrawal options drop-down box.

Once you've reached this point you're set. You can now repeatedly withdraw fiat currencies to that account. Just enter the amount you want to withdraw and provided you have that amount in your MtGox account it will be withdrawn and deposited into your bank account within a day or two.

**OKPAY** - To withdraw fiat currencies using OKPAY is easy. You will have to create an OKPAY account on their website. It is much like Paypal and creates a digital online account that you can manage yourself. It can be linked to your local bank account for withdrawals.

A screenshot of a 'Withdrawal Center Wizard' window. It has a title bar with 'Withdrawal Center Wizard' and a close button 'X'. The form contains two input fields: 'Label:' with the text 'IdiotsGuidetoBitcoin' and 'OKPAY ID:' with the placeholder text 'Enter your okpay ID'. At the bottom, there are two buttons: 'Close' on the left and 'Next >' on the right.

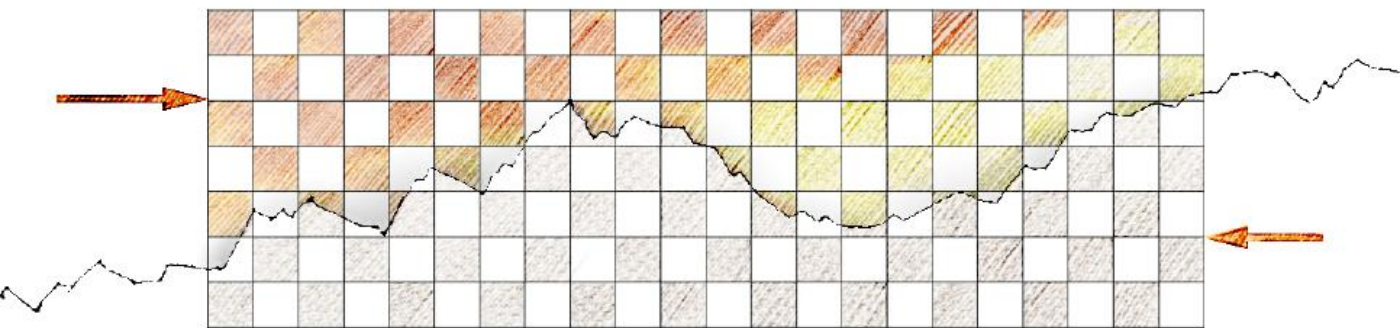
So once you've created an OKPAY account on [www.okpay.com](http://www.okpay.com) you simply choose a label (this will appear in the withdrawal options drop-down box) and enter your account ID which is your the email address linked to your OKPAY account. Then you're good to go. After the short verification period you will be able to withdraw funds to your OKPAY account. From there you can manage and withdraw your funds to your bank account.

So just to recap. It's easy to sell Bitcoins for fiat currency but gaining access to the cash just takes a little time the first time you do it. Thereafter withdrawing your funds is simple and quick.

Now that you've got the basics covered you can start trading. Happy hunting!

# Chapter 6

## Trading Bitcoin



**W**e've briefly discussed buying and selling Bitcoins as a way to invest and make money in the short term. Some people choose to do this more as a hobby, but more and more people are beginning to do this full time or even part time, and have been able to make quite a consistent income doing so. You've no doubt heard of trading in the stock market. Well, trading Bitcoins in the Bitcoin economy is not a whole lot different and has proven to be very lucrative.

---



## The Bitcoin Economy

The first thing you need to understand about the Bitcoin economy is that it is volatile, just like the stock market is. The price of Bitcoin can and will unpredictably increase or decrease over a short period of time. It's also important to understand that Bitcoin is incredibly young, at the time of this writing it's only four years old and it is just now beginning to become more legitimate and widespread – the mainstream is picking up on it to a point that it cannot be ignored.

At this point, it's safe to say that you shouldn't keep your savings in Bitcoin and it is, by all accounts, a high risk asset, but an asset nonetheless. We typically think of assets as something we own. A better definition of an asset would be something that makes us money. A car, for example, that you have to work to pay off, is not an asset – that would be considered a liability. However, if you purchased that car, and then rented it out, it would be an asset. Bitcoin is indeed an asset, but it's high risk in the sense that a number of things could take place.

Another virtual alternative currency could overtake it. So far, no other competing virtual currency has out-shined Bitcoin, but it has tried. It is a real possibility that another virtual currency could gain in popularity over Bitcoin, although it is rather unlikely since there are so many mainstream investors now putting their faith in this particular currency. A good way to think about this would be in precious metals and how, at times throughout history, silver has been sought over gold. You can think of Bitcoin as gold, and the competing alternative currencies as silver and bronze. At the time being they are currently worth money, and may grow in value, but they have not, as of currently, trumped Bitcoin in legitimacy or popularity.

Government, in any particular country, could seek to implement extreme oversight of Bitcoin, even going so far as to attempt to shut down exchanges. This could dramatically devalue Bitcoins.

Those are just a couple of examples. In the current sense, Bitcoin is not devoid of mainstream market psychology, which we'll get into now. When it comes to traditional market theories, we know that traders' behavior affects the supply and demand, which influences asset prices. This means that, in the case of Bitcoin's soar to popularity and sustaining

increased price value, the more faith people put into Bitcoin and the more mainstream investors keep clamoring to be a part of it, the more the value will rise due to its increased popularity. This is assuming that investors trade rationally according to certain types of assumptions.

The point at which issues arise comes about when a bulk of investors enter the market, which is happening now. This means that not all of those investors will behave according to the assumptions that they should be rational. On the contrary, many of them will behave according to their own rules and will react to outside information. This is why we call them irrational investors and traders. They will let something simple such as a tiny news report that seeks to devalue the Bitcoin affect them so terribly that they would exit the market in bulk, which would cause others to lose faith in the currency, and cause the price to plummet for other investors that decide to stay in the market. This is because these investors trade with their emotions and not with rational decision, while rational investors will make decisions according only to fundamental market theory.

All markets are largely behavioral, and we can see this in Bitcoin's recent surge in popularity and its surge in value. In February 2013 a single Bitcoin was worth about \$20. By the beginning of April, a single Bitcoin had surged to about \$250. Reputable news sources were covering this surge, but in the process, they labeled this surge as a bubble ready to burst. The positive feedback from news sources that the currency was increasing in value and that more investors were seeking it out caused more people who didn't know about Bitcoin to invest, but the subsequent fear of a bubble bursting paired with the misunderstanding of how exactly Bitcoin works aided in it dropping in value.

Another thing that happened was that MtGox got hacked and actually shut down its operations, which caused panic and further dropped the value of Bitcoins, which plummeted from \$250 to about \$60. At the time of this writing, Bitcoin has stabilized and has been hanging around \$115 to \$130 a Bitcoin, still much higher than it ever was before.

Because of the overwhelming amount of blogs, news reports, and information that has now reached the mainstream about Bitcoin, it has caused a wider array of potential investors and buyers into the currency to seek out information on it. Realistically, the fact that you're reading the book right now is a great example of this.

Because Bitcoin is highly volatile and is considered a behavioral economy, let's explore some of the ways in which individuals make decisions. These are very important to understand and as you go on trading you will recognize these effects in yourself and in others:

### The Psychology of Trading

**The Bandwagon** - This is a case of when a person just tends to go with the flow and it's not just confined to a market place effect, as you can see people do this everyday no matter what setting you're in. This is when individuals make decisions due to the expectations of the people surrounding them – most of us have done this. When the majority of people are acting a certain way, this individual will follow despite any personal beliefs they may have. You can see this when people buy something not because they need it, but simply because it's trendy. In a market sense, this can have a lot of consequences, as people will follow the majority based on unconfirmed information such as gossip, speculation, and more, which can cause prices to vary sharply.

**The Herd Mentality** - Picture a herd of cattle just sitting there, chilling out in the middle of a field, when all of a sudden one of the cattle hears something off in the distance and freaks out. That one cow, out of the entire herd, starts worrying and shouting and snorting and kicking the dirt, which freaks out two or three more of those around it. Then, before you know it, the entire herd is freaked out and running through the fence towards... who knows? This is kind of what people do a lot when it comes to the marketplace, and it's pretty similar to the bandwagon effect. However, in this situation, individuals act as a group without planned direction, which happens a lot during market crashes and market bubbles.

**Loss Aversion – Disposition Effect** - This situation commonly occurs when people would rather cut their profits and keep their losses. Typically, this is when investors sell their assets even when the price has increased, but will keep something that has decreased in value.

**Focusing** - Sometimes, when there isn't a lot of information available, people will tend to latch onto whatever small amount of information surfaces and rely on it, despite the fact that it is of small significance. This causes the investor to put all of their faith in a single piece of information

instead of a general solution. An example of this would be when the value of Bitcoin is going down, the investor hears one piece of positive information – even though it may be rather insignificant – and thinks it will change the price direction and allow them to profit.

**Optimism Bias** - This is when the investor tends to think everything is awesome all the time – the glass is always half full. These types of investors tend to put too much faith in planned actions resulting in overestimation of the likelihood of positive events. The problem is, they're so optimistic, they tend to underestimate the possibility of any negative consequences.

**The Ostrich Effect** - If you bury your head in the sand, no one can see you right? If you close your eyes, you're invisible...right? This is the ostrich effect, and it's pretty much just a case of denial. Typically, investors of very little experience fall into this particular facet by denying negative situations. They become so focused on their goal to make money that they do not accept the very real existence of current or future negative events.

**Overconfidence** - When everything is up, then it will just plain continue to go up no matter what, right? This is over confidence. No one can argue that confidence isn't a bad thing, but the overconfident investor is the one who believes that his/her judgment is flawless, despite the fact that their accuracy record doesn't demonstrate it. Of course, whenever this type of person receives an increase in profits, they tend to think that all of their past misjudgments are somehow inconsequential.

**Regret** -Regret isn't fun, especially in hindsight of an investment that you could have made, which would probably have netted you a ton of money. This happens when investors make a mistake in judgment, such as not selling a large amount of Bitcoins when the price was high by thinking that the price would go even higher, just to have it plummet in a few short hours. Or, it could come when the investor sells too soon, just to see the market value soar, which often negatively influences future trades.

When it comes to Bitcoin and its continued popularity and whether or not it will increase in value really comes down to the actions of investors. In order for BTC to become more stabilized, more and more investors need to not only put faith in it, but more and more individuals need to spend it regularly and make an effort to do so. By doing this, Bitcoin

continues to increase in value as it becomes more common. At the time being, the mentality is to hoard.

If you'll remember the beginning of this book, we talked about how many economists think that the fact the United States remained on the gold standard so long during the Great Depression was one of the primary reasons it lasted so long. Well, it wasn't so much the gold standard itself that caused the problem, it was the actions of the general populace who were hoarding their gold and assets rather than spending them that caused the Great Depression to last longer than it should have.

It is by spending currency frequently that you continue to give it value outside of the investment pool and it is also what provides stability. And, no matter what market you're in it is the way in which investors (that means you) act with their investments that dictate the entire future of any given market.

When it comes to trading Bitcoin and stabilizing the currency to make it a little less volatile, certain steps need to be taken.

Explore various exchanges – MtGox should not become a monopoly. By doing so it makes the entire economy vulnerable to an isolated attack. Remember, no smart investor puts all of their eggs in one basket. Just as any person who trades with non-digital currency knows to have multiple checking accounts at various banks, multiple investments, and multiple savings, any good Bitcoin trader will understand that they should store their Bitcoins in multiple wallets and trade through various exchanges outside of MtGox.

Don't just invest, SPEND – Think about this in terms of a credit card. You know that good credit is important because some day it will allow you to put a down payment on a house or a car or obtain a loan for a business. In order to have good credit, you can't simply get a credit card and not use it. On the contrary, you have to purchase things with that credit card and then pay it back on time and in full in order to build your credit rating over time. By doing this, you build faith among the credit agencies in that you are a responsible person who pays back any accumulated debt in a timely manor – this makes you a safe and worthwhile investment. Bitcoin isn't much different. In order to make Bitcoin a safe and worthwhile investment in other people's minds, then it has to be used more and more regularly. Which means that individuals investors need to spend it as much as possible, and not just trade it

amongst themselves. Just like a credit card – you don't need to buy big things in order to give yourself a higher credit rating, you may just go out and buy your groceries on credit once a week. With Bitcoin, you need to make sure you that you make a donation with it or buy a pizza with it – exercise your Bitcoin spending rights. By doing so, you add more value to the currency and collectively help to stabilize its growth. If you're a business owner, make an effort to accept BTC as payment and encourage your customers to get into it. The larger the BTC economy becomes, the more sustainable it will be and the harder it will be to destabilize.

### Bitcoin Trading Basics

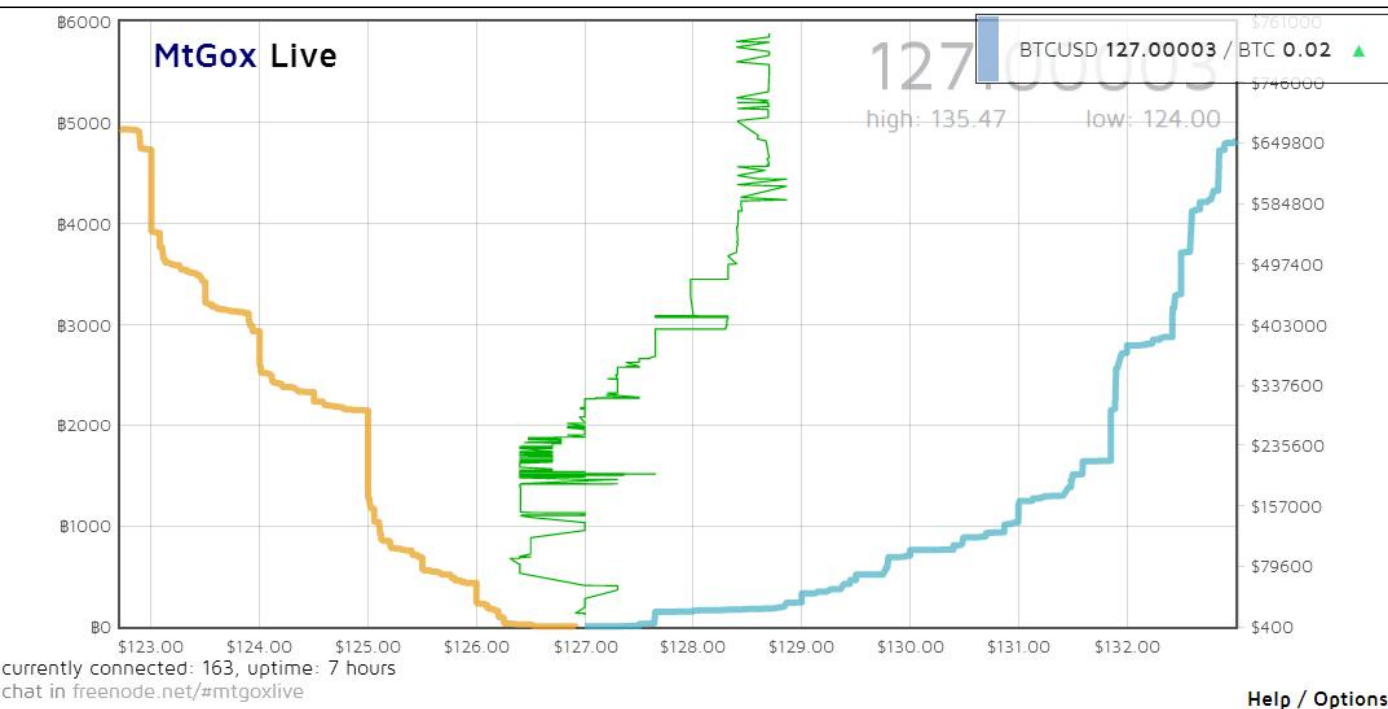
When people think about trading, images of the stock market are brought to mind – all of those screaming people, throwing around papers in a pit while suit-clad businessmen sit up top smoking their cigars. People think about giant computer screens filled with complicated charts and graphs, running numbers at lightning speed. It's enough to scare anybody out of ever doing anything with trading.

Fortunately, Bitcoin isn't so crazy and most definitely not as complicated. Anybody can trade Bitcoins successfully and it doesn't take some kind of financial savant to be successful. It just takes some patience, a few helpful tools, and a keen eye.

The most important thing you can do when Bitcoin trading is to keep on top of what the market is doing. In order to do that, you need to keep up with the current price of Bitcoin. There are a few great resources to help you do this.

## Live Bitcoin Market Charts

One of the simplest, most popular, and straight forward market charts is the MtGox Live chart (<http://mtgoxlive.com/>). Upon arriving, you will see three lines that form a V shape. The line on the left will be orange. The line in the middle will be green. The line on the right will be blue. In addition to that, you will see a  $y$ -axis (the left hand side of the chart with numbers represented in BTC) and an  $x$ -axis (numbers on the bottom showing USD – or whatever currency you decide by clicking the “Options” button on the far bottom right).



In the top left corner of the chart you will see the current price of a Bitcoin along with the day's highest price and the day's lowest price as well as live movement.

Right off the bat this may make little sense but it's actually pretty simple. First, let's look at what the individual lines mean.

**Orange Line (on the left)** – This represents the cumulative volume of outstanding bid orders. This shows market depth – how many BTC would need to be sold in order to move the price down to a particular level. Market depth is essentially the size of an order needed to move a market price in any given direction.



The Blue Line (on the right) – This represents the cumulative volume of outstanding ask orders. It shows how many Bitcoins need to be purchased in order to move the price of Bitcoins up.

The Green Line (in the middle) – The green line shows the historical price shifts in value that have been happening recently. It goes downward – the oldest being at the top, and the newest being at the bottom.



The above chart has four marked points, A, B, C & D.

Point A is marked along the orange line which represents outstanding bids, i.e. dollars on offer for Bitcoin. Point A corresponds to \$126.46 on the  $x$ -axis which means that the segment of line to the right of point A represents all the bids that are higher than \$126.46 per Bitcoin and have to be fulfilled before someone offering \$126.46 for a Bitcoin will have their order filled. The total amount of Bitcoins this represents is 1767 which corresponds to point A on the left  $y$ -axis. The total value of these orders is \$289,652 which corresponds to point A on the right  $y$ -axis.

Point B is the end of the orange line and represents the highest bid for a single Bitcoin. In this case \$133.13.

Point C is the end of the blue line and represents the cheapest Bitcoin on offer. In this case \$134.86. Point B and C are \$1.72 apart but as soon as they equal each other, which would see the blue and orange lines touch, an order is filled and someone buys a Bitcoin. However because this is instant the lines on the graph never actually touch.

Point D is along the blue line which represents the outstanding asks, i.e. Bitcoins being sold for a specific price. Point D corresponds to \$136.99 on the  $x$ -axis so the line segment to the left of point D represents all the Bitcoins on sale for less than \$136.99 per Bitcoin. Each of these will have to be sold before the Bitcoin at point D, on offer for \$136.99 will actually

be sold. And so the market price continually changes as bitcoins are bought and sold.

So transversely if you want to know how many Bitcoins need to be purchased in order for the price of a single Bitcoin to reach \$138. You simply look down at the bottom of the graph (the  $x$ -axis) until you find the \$138 mark. Then trace that up to where the blue line meets it. You then find the corresponding figure on the left  $y$ -axis. This will tell you how many Bitcoins need to be sold before they reach \$138. The right  $y$ -axis tells you what those Bitcoins are worth.

The same goes for price reduction. If you want to see how many Bitcoins must be sold in order for the price to drop, you simply look on the bottom of the chart (in descending order to the left) and pick the price point you want (let's say it's \$90) you trace that up to the orange line and mouse over it. This will show you how many Bitcoins need to be sold in order for the price to drop to that level.

However, your most important number is simply going to be the big one at the top right, which demonstrates the current price of a Bitcoin.

Another graph, that is much more in depth, and that many people find is easier to read, is Bitcoinity's (<http://bitcoinity.org/markets/mtgox/USD>)



What's great about this chart is that, in order to estimate market depth, you don't have to look at the bottom of the chart and trace it up in order to see how many Bitcoins need to be sold or purchased for prices to drop or rise. If you look at the bottom chart you'll see a similar V shape as the MtGox Live chart, with green on the left and red on the right.

If you mouse-over any point on these two lines you will see detailed information on how many Bitcoins need to be purchased/sold in order for prices to reach a certain point. This makes it incredibly simple.

Additionally, on the right side of the page, you are able to see a life tally of each Bitcoin price fluctuation along with its current USD/BTC value.

With Bitoinity's chart, you don't just have to keep up with MtGox's exchange. You can also choose to see how it's going on Bitstamp, BTCE, and Campbx exchanges by selecting from the options at the top. It's also very easy to switch between currencies.

Again, the most important thing to look out for is the current value of Bitcoins.

### Helpful Mobile Apps

Because the Bitcoin market is so volatile, it's important to stay on top of it in order to trade Bitcoins successfully. The only problem with that is most people can't sit in front of their computer 24/7 waiting for the market to move in order to take action, especially if you're trading Bitcoin on a part time basis or as a hobby while holding down a full-time job. Mobile apps are great with this, as many of them allow you to set notifications in case the market value of a Bitcoin goes down or up in your specific currency within your favorite exchanges. If the price dips way down, you'll know that's a good time to buy up some Bitcoins and if the price goes up, you'll know it's time to sell a few off for a profit.

Let's take a look at some options.

**Go Bit Go** – This is a free service that will text or email you when the Bitcoin price in your chosen currency hits a certain value, which you

pre-select. For example, if you want to be notified every time the price of Bitcoins goes up 20%, you can set that option. Alternatively, you can do the same if the price falls so that you are always prepared to act during important market changes. You can also be notified from with what's going on with various exchanges including BTC-E, Mt.Gox and Vircurex.

**CoinCliff** – This app takes a slightly different approach. It works similarly to an alarm clock. It will notify you of any pre-selected changes in Bitcoin prices. In addition to alarms, the app can also be set for regular notifications such as ones that are displayed when text messages are received. The CoinCliff app takes its data from Mt.Gox, but is planning on adding more exchanges such as BTC-E and Bitcoin-central.

**Bitcoin Paranoid** – In addition to this app displaying the current value of Bitcoin in USD it also supports alarms.

**Bitconium** – This app supports alerts and takes real-time information from the following exchanges: MtGox, Cavirtex (Canadian Virtual Exchange), BTC-E, Bitstamp, and CampBX.

Of course, these aren't the only apps available. Depending on the kind of smart phone you have, you can search your app store for similar apps that fit your needs.

### Forums and The Bitcoin Community

Now that you have the correct tools you need in order to keep on top of the Bitcoin market, it's important to always be involved in the Bitcoin community and the best way to do this is through various forums. All the tools in the world are not going to make you the best trader – in the end that all comes down to you. However, you can keep improving your skills by seeking knowledge from seasoned traders by finding out what they're doing and how they're doing it, asking questions, and seeking general advice.

There are a large variety of Bitcoin forums and online discussion communities, and just performing a simple Google search with "Bitcoin forums" or "Bitcoin groups" will return plenty of relevant groups, so we

don't want to tout any one community over another here. The best thing to do is become a member of multiple forums and stay involved with them.

Not only will being a part of these forums allow you to ask questions and seek advice, it will also keep you up on what's going on with the Bitcoin economy – what kind of major movements are traders looking to make, what kind of news is circulating the forums, are there any projected updates in the market such as big time investors helping Bitcoin gain more legitimacy or an issue that could possibly cause Bitcoin prices to lower in the next few days. These are the things that you must keep up with in order to be an effective trader.

The forums and other Bitcoin community spots throughout the Internet are also great places to buy items with Bitcoins and also services. Web developers and graphic designers, for example, often visit these forums offering their services and their willingness to be paid via Bitcoin.

### Set Your Alerts and Search For Info Daily

Being an effective trader is all about being informed. In addition to keeping your eyes open in the Bitcoin forums, you should also set your Google Alerts to notify you whenever articles, blogs, press releases, and other announcements regarding Bitcoin are published online.

Make sure to search "Bitcoin" in Google every morning or evening to see what kind of news pops up for the day.

### Buy low, sell high

All in all, when it really comes down to making money as a Bitcoin trader, it's about buying low and selling high. Regardless of your wallet, your chosen exchange(s), mobile app, and whatever charts you follow the most, you always want to make sure you buy low and sell high. Sometimes people tend to forget this is the simplest equation there is for a trader, and it all comes straight down to this important truth.

## Chapter 7

### Spending, Accepting, and Promoting Bitcoin



**A**lthough we've already talked a little bit about where you can spend Bitcoins earlier in this book, you may still be wondering just to what extent you can actually use Bitcoins to pay for stuff. For example, can you buy a cup of coffee? Can you purchase a movie ticket?

The fact is that, in reality, you can spend Bitcoins anywhere and you can spend them on anything – there is no limit whatsoever to what you can and can't spend Bitcoins on. This doesn't mean, however, that everybody

---

accepts Bitcoins as payment, and therein lies the problem. Bitcoin is such a new currency that it could become more and more popular at this point (as it seems to be doing) or it could be overshadowed by another emerging digital currency. Even though more and more locations are accepting Bitcoins both online and offline, it is still nowhere near the scale it needs to be in order to be a truly mainstream currency that is more stable due to legitimacy.

*There are a few ways you can approach Bitcoin at this point:*

- You could trade them and watch the market closely
- You could hoard them long term in hopes that one day they'll be the backbone of your retirement fund (which is actually a very real possibility – consider owning 100 Bitcoins that are worth upwards of \$5,000 each 40 years from now).
- You can spend them frequently and accept them as a form of payment, thus encouraging others to get into it.

Now, the first two options are fantastic, and you are most definitely encouraged to trade and save your Bitcoins through investment. But, one of the things a lot of people forget about is that spending Bitcoins frequently, accepting Bitcoins as payment (if you're a merchant), and generally encouraging the use of Bitcoins is the number one best way to continually legitimize the currency. It takes a collective effort on behalf of Bitcoin supporters to keep the momentum going with the currency, because the more people that accept it and the more normal it becomes to spend BTC, the more legitimate and stable the currency becomes, which makes short term trading and long term investment an even better decision on the ground floor.



## Spending Bitcoins Online

Because Bitcoin is a digital currency, the Internet is its natural environment, which makes your options for spending BTC much more plentiful in an online environment. Many online venues accept Bitcoin directly. However, even if they don't, you can always use resources such as the following:

- *Bitspend.net*
- *Bitcoinrunner.com*

Those two websites will allow you to buy anything online from any retailer even if they do not accept Bitcoin. Although there are fees involved, they are typically very low (under \$3 per order).

***www.opecoli.com*** - When you're looking to spend a Bitcoin this is the best place to start, they are the most thorough online directory of all merchants that accept Bitcoin. The website offers you the choice of online stores as well as physical stores so if you feel like a cup of coffee and would like to know if there is a local café that accepts Bitcoin Opecoli.com is the best place to start. I believe they are in the process of developing a smartphone app which will be great as bitcoin spreads.

(Its amazing what you can already buy for Bitcoins. So besides recommending having a look on Opecoli I've included a few interesting stores at the end of the chapter)

Whenever you're looking to purchase something online, also make sure to always look at the payment options and check whether or not they offer Bitcoin payments directly. Buying with Bitcoin is easy and fun, and remember, it helps further legitimize the currency, adding to its continued stabilization.

## Donating Bitcoins

Many charities are beginning to accept Bitcoin donations, which is also aiding in legitimizing the currency. Next time, when you want to donate to a charity, make sure to check and see if they accept Bitcoin. You may also want to consider this when contributing to a political campaign.

## Spending Bitcoins Offline

There are a growing number of offline retailers now accepting Bitcoin as payment, however there isn't a definitive list yet. There are companies such as <http://pizzaforcoins.com/> that are making it easy for people to purchase pizza with Bitcoins from major names like Domino's.

The best thing to do as a Bitcoin supporter is ask your local retailers whether or not they accept Bitcoin. When you find that a local retailer does not accept Bitcoin, tell them what it is and what it's about and urge them to accept it. This, again, will help spread the word about Bitcoin and open up more offline locations where it can be spent.

## Accepting Bitcoin as a Merchant

Perhaps the best way to build up your Bitcoin wallet and help stimulate and stabilize the Bitcoin economy is to accept it for payment within your own business, which is just about as easy as accepting PayPal or debit/credit card payments. Not only that, but encouraging people to pay via Bitcoin is a great way to help the currency.

Before we get into a few of the ways you can accept Bitcoin as a merchant, it's important to note that, because Bitcoin is currently very volatile, it's beneficial not to hold onto Bitcoin payments in Bitcoin form for too long, unless you're trading the Bitcoin or saving it long term. The reason for that is, once an item is paid for via Bitcoin, the price could drop. Fortunately, it's very easy to quickly exchange Bitcoin payments for cold-hard cash, which can be done directly on your smart phone, tablet, or computer via your chosen exchange.

There are fantastic overall advantages to accepting Bitcoin as a form of payment, because it gets rid of all of those pesky fees that come with credit/debit card transactions such as the following:

- Authorization fees
- Processing fees

- Sign-up fees
- Annual fees
- ATM fees
- Maintenance fees
- Compliance fees
- Overdraft fees
- Over-limit fees
- Minimum balance fees
- Late fees
- International currency fees
- Paper statement fees

Typically, if you use a Bitcoin merchant solution (there are a few very respected and trusted ones, that we'll list in a bit) there is only one low processing fee and that's it. Not only that, but Bitcoin is usually more secure than credit card payments because it's like paying cash for an item versus trading information that can be stolen by a third party.

Let's look at some of the ways you can accept payments as a merchant.

### Accepting Bitcoins via your Website

**Pre-Generating Bitcoin Addresses** - One way to accept Bitcoins as payment through your website is simply by pre-generating a large number of receiving Bitcoin addresses. This way, you don't have to go through a Bitcoin merchant provider utilizing APIs and third party services. When you use this option, you ensure that your web server never actually handles any of the Bitcoins. Instead, it just gives out addresses that belong to a wallet you maintain elsewhere (web wallet, mobile wallet, software wallet, or paper wallet). Additionally, by using a unique address for each order, you will always be able to know which payment belongs to a specific order.

In order to pre-generate addresses, there are a couple of tools you can use:

- **Pywallet**
- **Bitcoin Address Utility**

These utilities generate Bitcoin addresses with corresponding private keys. The Bitcoin addresses are loaded onto the web server and not the

private keys.

Using the Bitcoin software, you can check for incoming payments if you are manually shipping goods. You can also use Block Explorer or Abe to verify payments that you're about to ship.

However, for those who aren't technologically inclined, this method may be a little time consuming so a better option would be to use a third party application.

**Third-Party Applications** - Third party plugins are the equivalent of paint-by-number installations that are easy to setup and operate fluidly. They use shopping cart interfaces that automatically handle all of your Bitcoin payments. A couple of popular applications are as follows:

- **walletbit.com** – This application not only supports on-site checkouts with Bitcoin currency, it also includes mobile payment options.
- **Bitpay.com** – Bitpay is quickly becoming one of the most popular options for merchants to accept Bitcoin as payment, whether you're a retail business, ecommerce business, charity, or contractor.

These applications make it easy to set yourself up to receive payment in BTC. If you get confused or need help, you can also contact their support desks and each installation comes with detailed instructions.

### Accepting Bitcoins Via Mobile Apps

Most third party applications, including the ones listed above, have options to allow for mobile Bitcoin payment. For businesses that are primarily brick and mortar, having an app for your mobile device is indispensable and also very simple.

Let's say you own a coffee shop and someone wishes to pay for their coffee via Bitcoin. Your payment system (for example BitPay or WalletBit) offers a mobile application that's easy to setup. You simply input the order into your mobile app and it generates a QR code that

your customer scans (exchanges such as MtGox all have mobile apps and allow QR scanning for mobile payments). The entire process takes less than a minute and isn't much different than someone paying with a debit/credit card.

### Interesting stores that accept Bitcoin

- **Bitcoinin** – Books, Movies, Consumer Electronics, Food, Beverages, and more added daily and upon request
- **Bitcoinblaster.com** – Consumer Electronics in Bitcoins - Laptops, desktops, tablets, digital cameras, televisions and more! Inventory added all time.
- **BTCgadgets** – Buy cheap products with your Bitcoins! Free shipping worldwide.
- **Gadgets Direct** – Over 20,000 Gadgets all with Free Worldwide Shipping now accepting Bitcoins.
- **Säkra Dörren** – Over 4000 security products such as locks and alarm systems shipping worldwide. Based in sweden.
- **SurplusTraders.net** – The World's Leading WHOLESale Liquidator of Factory Excess Technology Parts & Equipment.
- **JJGames**, – used video games and consoles (5% discount for Bitcoin purchases)
- **BMIgaming.com** – Arcade Games from BMI Gaming, the "World's Largest Gaming Superstore" offering delivery to over 90 countries worldwide
- **Noella Jean Jewellery** – Bracelets, earrings, necklaces and rings.
- **Something Geeky, Appealing to the inner geek** - geek t-shirts, hoodies, mugs, bags, sweatshirts and more
- **Patcht**- Custom clothing that involves you in the design process.
- **Bucarelli**- iPad and macbook leather cases
- **Ico6**- Geek Shirts & Bitcoin Apparel: Dressing all Einstein's and Beyond!
- **All Things Luxury**- Vast selection of luxury jewelry for less. Earrings, necklaces, pandora style beads, simulated diamond engagement rings and much more. Up to 75% off retail, plus all items ship for free.
- **Shirtalicious UK**- A selection of quality T-Shirts with Free Shipping.
- **BTCZone.com** - Bitcoin ecommerce - An online store that lets you search for products in many categories and accepts bitcoins. Free shipping on many orders.
- **Luana's Bijoux**- A Bijoux store. Currently sells earrings and bracelets.
- **R-Shirt**-Accepts Bitcoins for geeky pirate R-Shirts.
- **Robots Never Die**
- **The White Peacock**, Gothic Lolita clothing for Bitcoins
- **Og Dogg Records**- Hip-Hop music site accepting bitcoin payments

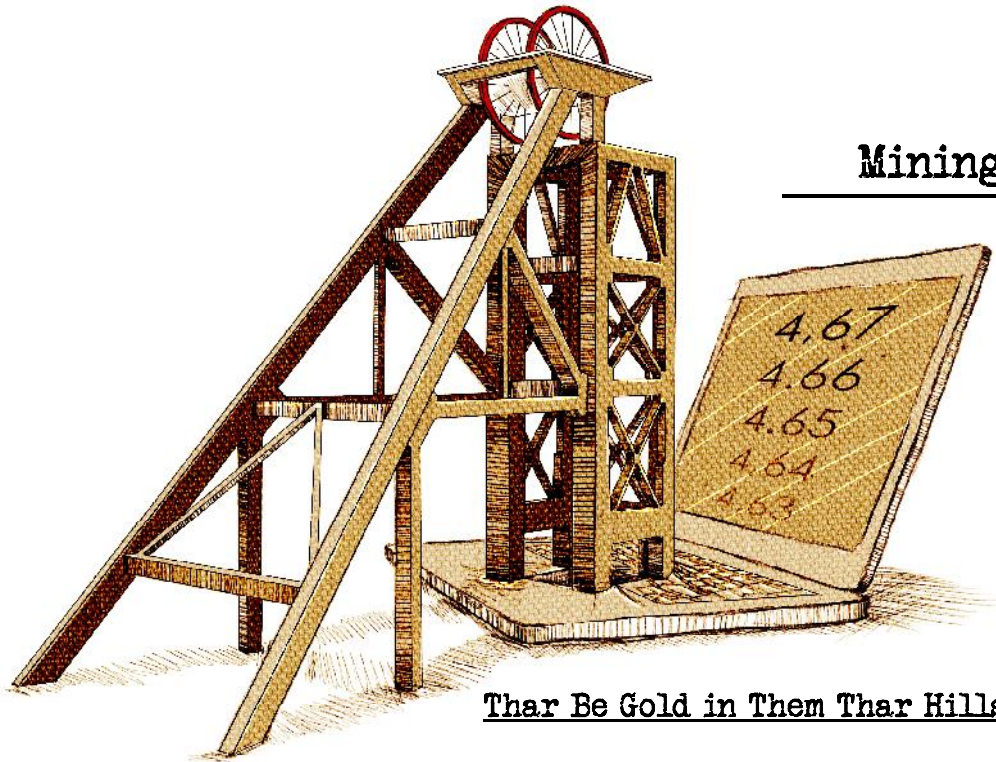
- for T-shirts and other Hip-Hop related merchandise.
- **From Heart to Heart**- Unique, hand made jewellery. A special gift for yourself, your wife or your girlfriend.
  - **Poppyluce**- Custom crafted jewellery and accessories
  - **Bitcoin Team on Etsy**- Etsy merchants accepting Bitcoin
  - **Windfire Chainmaille**- Chainmail jewelery.
  - **HeatSlingers.com**, "Simply put, we are sneaker heads. We're just sneaker collectors who are sick of the eBay nonsense" Email for info on payment w/Bitcoins
  - **The Gentle Pony**- T-Shirts with weird jokes
  - **T.S. I Love You Hats**- Each T.S. I Love You hat is a one of a kind, hand-created piece, re-worked and assembled from precious old bits...
  - **Dri-ApparelSports clothing**, tee shirts, shorts, pants, hats, and totes.
  - **Soccer Uniforms** – Soccer shirts, shorts, socks and accessories, including customization services.
  - **ZAS robapinzas.com**-- Hippie Ethnic Alternative, clothes and much more... Shoes, accesories, piercing, decoration items. Wholesale and Retail (Accept bitcoin for wholesale customers).
  - **SurvivalFood.com** – Emergency and survival food storage supplies, including freeze dried food and MREs.
  - **Joseph's Garden** – Open-pollinated landrace garden seeds.
  - **Fine Things Store** – Fine Things for your house and your family. Silver, Glass, Antiques.
  - **Nestorgames** – is an independent publisher of portable board games. More than 60 titles in its catalogue.
  - **Arimaa** Game Set, an animal themed board game designed to be hard for computers, but easy to learn and intuitive for humans. Offers \$10,000 challenge for programmers.
  - **Blue Canary Night Light**, blue canary night lights
  - **The Critter Casual** --pet wear
  - **Telepienso** – Dog and cat food, top brands (Royal Canin, Hill's, Acana, Dr. Pet) Delivery to Spain, Portugal and Balearic islands
  - **Dr. Pet dog and cat food** – natural dog and cat food.
  - **A Curbing Edge**, Decorative Landscape Curbing in the greater Orlando Florida area
  - **Small Happy Eagle Enterprises**- Selling specialty incense.
  - **Azurerocket Design Studio** – Cut vinyl decals for indoor and outdoor application. Accepts custom orders.
  - **Keystone Pet Place** – Pet food and supplies.
  - **TorGuard Store** – DDWRT VPN Routers, HDTV Boxes, Android, NAS, Networking Accessories, Pre-Paid VPN Service and more!
  - **7Del.net**, Electronic Cigarettes
  - **AGNQ Tech**- Computers and computer components for sale
  - **Bitcoin ecommerce**- An online store that lets you search for products in many categories including electronics and accepts bitcoins. Free shipping on many orders.

- **Bitcoinblaster.com**-Consumer Electronics in Bitcoins - Laptops, desktops, tablets, digital cameras, televisions and more! Inventory added all time.
- **Bitcoinstore** (info) Over 500,000 products. The world's largest Bitcoin only super store. Consumer Electronics, Computer systems, PC components, Laptops, TVs, Hard Drives, RAM, Cameras, Network parts.
- **BitElectronics** - Consumer electronics. Hundreds of products: PC components, tablets, cameras etc... Worldwide shipping!
- **BitLasers**, Handheld lasers and laser accessories.
- **BitVapes**, Electronic cigarettes (e-cigs), starter kits, replacement parts, accessories and nicotine e-liquids.
- **CellPhone-Jammers.com**, Cell phone, GPS, GSM, 4G, Wi-Fi, Bluetooth, UHF jammers
- **CompSoul.com**—Sale of Computer Components, Systems, Electronics and More from Brand Names, Unique and Generic. Worldwide shipping available. Multiple payment options.



## Chapter 8

### Mining Bitcoins



#### Thar Be Gold in Them Thar Hills!

**M**ake no mistake about it, what's going on with Bitcoin right now is a veritable gold rush. In fact, the characteristics that defined the famed gold rushes throughout early United States history – and the various gold rushes throughout the history of the world for that matter – are nearly identical to what's happening with Bitcoin. However, instead of poor, dust-faced families traversing the country armed with pickaxes and a dream, we're faced with geeky techies covered in a spool of wires, armed with towers of whirring computers and blinking lights as they sweat profusely in an over-heated basement waiting for the next

cryptographic hash to be solved in exchange for a new Bitcoin.

People are going out on a limb and spending thousands of dollars on the latest technology and the highest computing power while running up monumental electrical bills so that they can mine just two or three Bitcoins a week, which at current prices would come to about \$1,200 a month. Not only that, but the more Bitcoin miners there are, and the more complex the mining rigs and operations become, the more and more difficult it is to mine. This is the setup.

Bitcoin mining was created to be a purposely arduous affair. It was not designed to be easy in any sense – it's a constant race to build better and better hardware to mine and it takes increasingly more startup money in order to build mining operations. As time goes on, this will only increase. Which means that the little guys with nothing more than a laptop and not a whole lot of technical knowledge are left in the dust (or at least they're left to trading Bitcoins by buying low and selling high rather than mining them).

However, for those who really want to spend the time to build mining operations and join mining pools (we'll talk about that in a moment) it can be incredibly lucrative. Depending on how good your mining operation is you can make \$20 a day or \$8000 a day (and yes, there are people making that figure on a consistent basis).

### How Mining Works in a Nutshell

There are a lot of heavy specifics that could be illustrated regarding mining and how Bitcoin works on the internal level. However, in order to mine Bitcoins, a uber in-depth knowledge isn't essential. Just like you don't have to be an economist or an expert financial forecaster in order to make decent money as an investor or trader, you don't need to know all of the internal technical workings of the Bitcoin mining process in order to actually mine them. So, here's your semi in depth summary of how Bitcoins are actually mined.

Picture a field with thousands of small houses scattered across it. Each house has a lock on the door and, in order to get inside, you have to figure out the combination. Inside each of the houses is a small treasure.

If you can figure out the combination, then you can get the treasure inside.

In regard to Bitcoin, the field is the Internet and the little houses are the "blocks" scattered across it. Each block is encrypted with cryptographic hashes that require complicated mathematical problems to be solved in order to be unlocked. Each time one of these blocks is unlocked, a Bitcoin is awarded for the effort.

These blocks are unlocked by downloading a software application to your computer, that uses your computer's problem solving capabilities to try and crack the cryptographic hashes in exchange for Bitcoins.

Now, imagine that those little houses were very easy to unlock at the start of the field. You could just try out a few combinations off the top of your head and unlock the door to get the reward inside. However, more and more people kept finding out about this great field where you could just walk in, figure out a lock combination, and get free money.

As this happened, and more and more people began showing up in this field to unlock the houses, the combinations got harder and harder and harder, which means they took more time to solve.

This is exactly what happens with Bitcoin – the more people that join the network and start mining, the more competition there is to solve the cryptographic hashes, this increases the difficulty of mining blocks across the entire network, which means more and more computing power must be used. That little laptop doesn't work anymore. Later, we'll talk about the kinds of hardware people actually use to mine Bitcoin, but right now suffice it to say that one needs a much larger amount of resources in order to get started. Think of it as people walking into the field with lock-picking technology and then complicated calculating technology, and so on, putting to shame all of those who used to just guess at the lock combinations.

Can you make a lot of money as a Bitcoin miner? The answer is most definitely yes, but it's an uphill battle and it will always get more and more difficult to continue making a high amount of money on a regular basis. Of course, this also depends upon the value of the Bitcoins themselves. If you're mining only two Bitcoins a week, but an individual Bitcoin is worth \$3,000 you're not doing too bad. But, if those Bitcoins are only worth \$117 as they are at the time of this writing, then it you will want to

reinvest that money into more hardware to increase your capacity to mine Bitcoins faster.

A new block is appended to the block chain via mining every ten minutes. Each time a block is mined, 25 Bitcoins are awarded. When Bitcoin was first made, the Bitcoins were awarded at a rate of 50 every 10 minutes each time a block was mined. However, every four years that figure is cut in half, which is why it is only 25 now. Four years from now it will be 12.5 Bitcoins every 10 minutes per mined block and so on until 21 million Bitcoins are in circulation in the year 2140 (of course, you're not going to be around at that point... unless you're a cyborg, then that would be just plain cool).

### Bitcoin Mining Hardware

When it comes to hardware, the most important thing you should take into account is the hash rate (that's a measuring unit of processing power – it's the rate at which your hardware can make intensive mathematical operations in order to mine Bitcoins). The higher your hash rate, the more Bitcoins you will mine in a 24 hour period.

In order to mine Bitcoin effectively at this point, you need a dedicated rig. Now, it may sound strange to call it that, but when you mine Bitcoin you're literally creating a piece of hardware with a singular purpose – to mine as many Bitcoins in a 24 hour period as possible. This entails creating a computer with a simplified motherboard that has a sophisticated cooling system (often these types of rigs are not confined inside a box so they don't overheat) and a lot of high-end graphics cards (GPU) where the computer draws its processing power from in order to mine coins.

People for the most part have been making their own mining rigs by purchasing the hardware needed and putting it together, creating stacks upon stacks of rigs. Each rig costs about \$900 to \$2,000 and drives electricity bills up very high as it sucks so much wattage from the grid. Not only that, but any room these rigs are housed in can become incredibly hot because they're running constantly.

However, at the time of this writing, brand new ASIC (Application Specific Integrated Circuit) that was in development for years has just

come to light. This technology means that purpose-built, permanently programmed chips with the application printed into the chip at the time of the manufacture is available. Essentially – these are Bitcoin mining rigs that you can buy rather than make. They have a predetermined hash rate, use far less wattage which lowers the electric bill, and makes it to where more people can mine bitcoin effectively.

The two companies that offer ASIC mining rigs are as follows:

**Avalon Asics** (<http://launch.avalon-asics.com/>) – This company has a great track record of actually delivering their rigs on time. The problem is, at the time this book is being released, they only take limited orders in batches and typically those orders sell out in less than 20 minutes. This will most likely change in the future, but right now it's incredibly difficult to obtain one of these. There are people who sell them on Ebay, but for much, much more than its original price (people are paying \$30,000 for a rig that originally cost \$7,000).

**Butterfly Labs** (<http://www.butterflylabs.com/>) – There has been a substantial amount of buzz going around Butterfly Labs, but with that buzz has also come a lot of frustration. Their products look amazing – incredibly low voltage, surprisingly affordable, stackable Bitcoin miners with various hash rates (from 5 gigahashes per second (GH/s) to 1,500 GH/s at the time of this writing). The only problem is that tons of people have pre-ordered these miners (over a thousand a day at some point) and very few have actually received their products. At this time, they are being released slowly. The longer it takes to receive the Bitcoin miner, the more complicated it becomes to mine Bitcoins, which means that someone who purchased a 25 GH/s miner several months ago will see themselves mining far less Bitcoins by the time it arrives.

Now that just about anybody is able to purchase their own Bitcoin miners in bulk due to these ASIC rigs without having to have a lot of technical know-how in order to build their own, it will boost the overall mining difficulty for the entire Bitcoin network, especially when you consider how many orders are coming in to both of the above listed manufacturers.

This isn't to say that Bitcoin mining won't be lucrative. Many of these investments will pay for themselves within a couple of months and they'll keep making money as time goes on. If you want to be a serious miner and you're in it for the long haul, you can keep investing new equipment.

Of course, the best thing about mining is that it all runs on its own – there is very little management on your part, especially now with these pre-made miners, there won't be any crashes or barely any upkeep. You'll be able to make consistent money everyday while you're sleeping. And, when it really comes down to it, that's the dream right?

Assuming Bitcoin continues to increase in value, becoming more and more legitimate over time, amassing Bitcoins now via mining could very easily make a lot of millionaires, as we're already beginning to see.

### Bitcoing Mining Software

Bitcoin mining software is fairly straightforward – is the software you need to install on your rig that works to solve the cryptographic hashes. There are many bitcoin mining apps out there including the following:

- **50Miner** – A GUI frontend for Windows(Poclbm, Phoenix, DiabloMiner)
- **BFGMiner** – Modular FPGA/GPU miner in C
- **BTCMiner** – Bitcoin Miner for ZTEX FPGA Boards
- **Bit Moose** – Run Miners as a Windows Service.
- **Poclbm** – Python/OpenCL GPU miner (GUI(Windows & MacOS X))
- **Poclbm-mod** – more efficient version of Poclbm (GUI)
- **DiabloMiner** – Java/OpenCL GPU miner (MAC OS X GUI)
- **RPC Miner** – remote RPC miner (MAC OS X GUI)
- **Phoenix miner** – miner
- **Cpu Miner** – miner
- **Ufasoft miner** – miner
- **Pyminer** – Python miner, reference implementation
- **Remote miner** – mining pool software
- **Open Source FGPA Bitcoin Miner** – a miner that makes use of an FPGA Board
- **Flash Player Bitcoin Miner** – A proof of concept Adobe Flash Player miner

## Mining Pools

The last lesson in Bitcoin mining is that you should always join a pool other miners, unless you have a ridiculously powerful mining operation and if that's the case you wouldn't be reading this book. Mining pools make it easier to get Bitcoins more consistently. Essentially, it's a bunch of miners pooling their resources, and sharing the spoils.

Mining pools offer shares – a hash is easier to create with a pool than solo, and it still provides proof that you have done valid work toward finding the next block. The more shares you can calculate and submit, the more fractional ownership you achieve in the next block reward (Bitcoin reward). Mining pools provide websites with stats and account management, which makes it easy to connect and monitor your hashing power and BTC generation.

There are many mining pools out there available for you to join, and unfortunately we can't tout any one over another within this book. However, a simple Google search for Bitcoin mining pools will get you started.



## Chapter 9



### Questions & Concerns

I'm Afraid Bitcoin will be hacked – everything can be hacked!

**T**his is one of the most common concerns regarding Bitcoin, so let's clear this up really quick. Can Bitcoin be hacked? The answer is no. Although it's arguable that the Bitcoin network has "some possibility" of being hacked (as does any entropy-dependent mathematical cryptography) the mathematics involved are far too absurdly improbable. You'd be better served coming up with 10<sup>th</sup> planet apocalypse theories than being worried about the Bitcoin network being hacked.

---

Quantum computing could theoretically change the validity of the current state of the art cryptography, but nobody has yet conceived of the mechanism by which any of that stuff would be possible. Even so, by the time quantum devices become truly useful, there will have been plenty of time to move on and newer, stronger currencies will have been devised.

The other thing is that Bitcoin has already reckoned on these eventualities and built in self-defense mechanisms, which increase the mining difficulty over time in response to the frequency of bitcoins being successfully created (which we have established throughout this book is a process that involves computationally-hard number-guessing, which automatically increases in difficulty every time a node in the network stumbles upon a valid solution whereby results are verified by the rest of the network and invalid unless there is a consensus).

Because the Bitcoin network is made up of thousands upon thousands of computers throughout the globe (this is the mining and trading network) a hacking group would need to synchronize a take-over of an overwhelming majority of the nodes in the peer-to-peer network, which is only theoretically popular in a Lex Luthor from Superman sort of way. But, in all honesty, it is more unlikely to occur than Walt Disney re-awakening from his cryo-sleep and being unanimously nominated King of the United Nations – it's possibly, but don't count on it occurring in your lifetime.

In order for Bitcoin to be truly shut down – the entire Internet as we know it would have to be completely cut off, which would most likely involve a world-wide infrastructure collapse, the likes of which would render all currency unstable anyway.

However, what CAN be hacked are wallets and exchanges. It's vital to discern the difference, because there are already many news headlines that read, "Bitcoin has been hacked!" Which scares people from investing in Bitcoin and scares traders into selling off their Bitcoins. Whenever you hear that Bitcoin has been hacked, first of all understand that it has not in fact been hacked. This is the equivalent of a news report coming out saying, "The Federal Reserve has been robbed!" When all that happened is a small bank in North Dakota got knocked over by a couple of burglars. It's nonsense.

Just like using your credit card to pay for items online or sending a check

through the mail, people can steal your money a number of ways and this is no different with Bitcoin. Bitcoin exchanges such as MtGox can be hacked and have been hacked. People's web wallets, mobile wallets, and software wallets can and have been hacked. It's up to the user to take necessary precautions to protect their Bitcoins by using paper wallets and encrypting their wallets while not keeping large stores of Bitcoins within exchange wallets.

### Will The Government Shut Down Bitcoin?

Another very big concern for many people is the possibility of the US government (or any other government) shutting down Bitcoin within the currency by dubbing the currency illegal. First of all, any government would be kicking a nasty hornet's nest by trying to impede the use of Bitcoin at its current level of adoption, because it would open up the same discussion for all other virtual currencies by definition, many of which are already backed and used by very powerful corps, and Bitcoin is quite defensible compared to all of those.

Money, by definition, is controlled by the people who agree upon its worth. If they want to tax and regulate it as real money, fine, and this is actually what is happening in most places – governments are working with Bitcoin. The technology of Bitcoin actually makes that easier to deal with than regular currency, and increases its validity overall – if the government works with Bitcoin, the currency grows in value because there is more faith in it.

However, the fact is that it is very scary for governments that Bitcoin is not bound by international borders and that it can be exploited for purposes such as money laundering, even though the currency is technically more traceable than dollars. At current, however, governments seem to be working nicely with Bitcoin and this reality is likely to continue.

The great news is that no government entity can actually shut down Bitcoin even if they tried. Just like a hacker group is unable to hack Bitcoin, a government can't shut it down. In fact, even if every government in the world teamed up with the soul purpose of shutting down Bitcoin, the chances that they would be able to do so is incredibly slim (in other words, virtually non-existent). Again, the entire Internet would have to be shut down completely in order for that to happen.

What the government CAN do to hurt Bitcoin is shut down exchanges or stop certain payment companies from allowing transfers to exchanges. For example, the government could shut down Dwolla, making it impossible for people in the US to transfer money from Dwolla to Mt.Gox. Or, they could put pressure on banks to refuse direct bank transfers to places like Coinbase.com or MtGox.

None these actions will destroy Bitcoin, nor will it shut down the exchange of Bitcoin. What it will do is serve to devalue the currency and cause people to lose faith in it. But, there will always be ways to easily exchange Bitcoins into currency and there will always be ways to buy Bitcoins easily. Another factor that's important to understand is that exchanges are located all throughout the world and new ones are coming up everyday, it's impossible for one government to control all of them unless each government cooperates to put a strangle hold on global exchanges.

So, can the government shut down Bitcoin? They can do a lot of damage to its reputation and cut off certain exchanges and locations where Bitcoins are bought/sold, but they can't completely bar you from Bitcoin or shut it down.

It's important also to keep calm when news reports surface such as, "The IRS Seizes Bitcoin Exchange" and so on. Again, this is the equivalent of the IRS looking into a banking scandal in a small town and the newspaper stating that the value of the American dollar is about to plummet because of it. It's simply not true. It's natural for various problems to arise between government and Bitcoin, especially as Bitcoin continues to soar in value and use. However, these small skirmishes should not be misinterpreted as some kind of major blow to the currency, and acting like it is only helps add to the problem.

### Bitcoin is Just a Bubble Waiting to Burst / Bitcoin is a Fad and Will Fail

First of all, you will hear often about Bitcoin bubbles. The thought that Bitcoin is a bubble like the ones we saw with the sub-prime mortgage meltdown, is simply not true. Bitcoin is a currently volatile currency, which means it is susceptible to huge shifts in value – it could go way up and it could go way down. Recently the media tends to label this as

“bubbles.”

As far as Bitcoin being a fad and failing – that's yet to be seen. One thing is for certain, Bitcoin is most definitely here to stay and cryptocurrency itself is no fad. At this point, cryptocurrency has taken off to such an extent that, if Bitcoin fails for whatever reason, another alternative cryptocurrency will replace it popularity.

The danger to Bitcoin isn't so much its validity and it certainly won't fail because it's a “fad.” What may cause Bitcoin to go under is being surpassed by another cryptocurrency. In this sense, it's important to understand a little bit about recent Internet history. Typically the way things go is someone innovates, then that innovation is improved upon is overtaken.

We can see this with the invention of Napster. This paved the way for peer-to-peer file sharing, and single-handedly changed the way we listen to music, share music, and subsequently how the music industry itself operates. Like Bitcoin, it was very worrisome to the entire media empire (in the Bitcoin sense, replace media empire with government and centralized banking). Eventually Napster was shutdown, and Kazaa took its place. Kazaa was like Napster in that people could share files such as music, movies, and software, but it improved upon Napster. Then, Bittorrent came along and changed the game forever and torrents are now the current standard.

We can also see this with social media. First there was Livejournal and Xanga where people would write blogs and others could comment on them easily, but both of these quickly turned into individual communities. Then came Friendster, which was the first social media profile site the web had ever seen. It was then over shadowed by MySpace, which stood as the king of all social media networks until Facebook trumped it. To this day Facebook is the most popular social media network – although there are others like Twitter and Google +, they play nicely with Facebook. The saying is that everybody on Twitter and Google + are on Facebook, but not everybody on Facebook are on Twitter and Google +.

Bitcoin is still susceptible to something similar. It's the first ever solid digital currency ever successfully conceived. Although there is no fundamental flaw in how it works, there have been other cryptocurrencies that are competing with it. At the time of this writing, none of those other

currencies are accepted to the level Bitcoin is and none of them have ever gone above \$4.

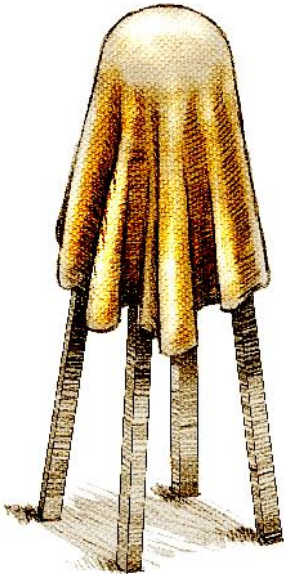
There is still a possibility that, at any time, one of these other currencies could gain in popularity over Bitcoin or that a new currency could come out that has some major improvements over Bitcoin and gains in popularity. This isn't anything to worry about. Simply paying attention to the market will help you avoid any major losses should Bitcoin begin losing popularity or value. Not only that, but Bitcoin exchanges into the other currencies and vice versa, which makes them play nicely together while still competing. Remember, competition is good.

Here are a list of the other currencies:

- Litecoin
- PPCoin
- Namecoin

All of these are accepted through various exchanges such as BTC-E and interchangeable with each other.

## Chapter 10



## Conclusion

**B**itcoin is quite literally changing the world. Although it's too early to tell the future for certain, one thing is for sure – cryptocurrency isn't going anywhere. Whether we see people with Bitcoin fifty to a hundred years from now is still yet to be seen. However, there is no doubt that Bitcoin has paved the way for a new people's currency – not one confined by location or government or central bank, but one that crosses borders and all cultures.

---



Just like how the Internet has already changed the way people are able to get information and communicate with each other on a global level – a change that will most likely last forever – Bitcoin is now changing the way our economy works, how we pay for things, and how we regulate currency. The Internet opened everything up for us – it allowed us free access to as much information as we wanted, breaking the monopoly that formal education institutions had on the control of information, allowing anyone anywhere to learn anything at anytime. It's a communal aspect of sharing and knowledge and change that has forever changed our culture for the better. It's only natural that the next step in that process be a new currency born out of such a revolutionary game changer as Internet.

Although Bitcoin may seem scary for a lot of people or may be initially confusing, it's always better to embrace it. Just as things like email and web browsing and online video and online banking and smart phones seemed scary and new at first, once these technologies were embraced, it no doubt added value to your life.

So, don't be afraid of Bitcoin, embrace it now and be a part of the world's first ever decentralized digital currency, and a new dawn in how we think of money.

*Thank you*



The Idiot's guide to Bitcoin...

---