Table Of Contents

Introduction

At the time of me writing this, Bitcoin is in a bit of a "recession." We are a couple of months after its meteoric run up to 20,000 USD per coin, but currently, the public doesn't care about Bitcoin. The average person, if they even know about Bitcoin at all, thinks it was a fad. They believe that by using or investing in Bitcoin, you're taking a massive risk because everyone that they know that also invested has lost thousands of dollars. Here's the thing, they're not (entirely) wrong.

What did you think, I was going to pull the wool over your eyes?

Bitcoin--and cryptocurrencies more broadly--are incredibly risky assets. I am not a snake oil salesman here to make you invest your child's college fund into Bitcoin. This is an emerging technology, and with that comes a lot of risk.

But guess what? We have only seen the beginning.

I am writing this book because I am confident that this is not the end of Bitcoin. I am writing this book so that you as the reader will be able to understand what the "big deal" about Bitcoin is. So that you can impress your partner, family, and friends with your understanding of the topic.

By the time you finish reading this book, you will understand the significance of Bitcoin, its purpose, and have a general understanding of the blockchain and other “altcoins” (cryptocurrencies other than Bitcoin). This book will be written in layman’s terms, but I will not sacrifice the quality of information. You can be confident that when you’re finished reading it, you will have a strong working knowledge of the technologies at hand, and that you will not be fooled by any charlatan trying to sell you a scam or condescend to you due to their supposedly superior intelligence.

Chapter 1

What Is Bitcoin?

Direct Answer: Bitcoin is a digital currency based around cryptographic algorithms.

The Bitcoin *whitepaper*[1]—the document that introduced Bitcoin to the world—written by "Satoshi Nakamoto," defines Bitcoin as a "peer-to-peer electronic cash system." There are debates as to who Satoshi Nakamoto is, and whether it's even one person, but all of that can be discussed later.

Underneath the hood, Bitcoin is simply a system of rules that, by using *cryptography*, allow for two users to transfer value without a third party authority. Basically, just like email allows for two people to send messages directly to one another, Bitcoin allows two parties to send money directly to one another.

That can't be all there is to it though, right? Something that simple wouldn't generate the kind of fervor that Bitcoin has created. It wouldn't make your coworker talk about it

endlessly, right? There's truthfully so much that we need to cover, so I'm just going to start from the top.

Where Did It All Begin?

Depending on how old you are, you may remember the late 90s dotcom boom. Around this time, an application named *Napster* showed up. This application allowed--or maybe allows, not sure if it's still around--users to put music online that other users could download quickly, but also...illegally. The website immediately faced a massive backlash and was eventually shutdown (to our dismay). As time went on, alternative applications such as Kazaa, Limewire, Bittorrent, etc. were created. All of these are what we refer to now as *peer-to-peer networks*.

If you don't know what any of these are, don't worry too much about it. Just know that this is where our blockchain story begins.

While you might have had a great time jamming out to AFI with your obnoxious haircut that demonstrated just how "non-conformist" you were, inadvertently you were also participating in a decentralized network. What makes decentralized technologies so interesting is that they do not have to be run through a trusted authority.

Historically, computers connected from client to server.

There was some massive warehouse (in a place with reasonably priced real estate costs) that was filled wall-to-wall with computers. These *servers* held all of the information that you would download onto your computer. Similarly, you could upload information from your computer to these servers.
When Napster was created, Sean Parker popularized the peer-to-peer network. Instead of going through a centralized authority like a record company, users could upload music to the network and other users could then download the music to their computers for free. Each computer held a little bit of the data in the network, providing a little bit of the content that made the network work.

While the peer-to-peer technological advancement was negatively received by bands like Metallica (still the least-metal thing they've ever done… well, excluding Load and Reload), it also allowed for Radiohead to receive worldwide acclaim and reach the Billboard 200 for the first time with their album Kid A.

Bitcoin is a *peer-to-peer electronic cash system*

Now that we have addressed the peer-to-peer portion, let's talk about a "cash system."

I can see you now, rolling your eyes at me. Tasheme, I know what a cash system is. Yeah, I know, it should be intuitive, but there are some underlying rules, that are

rarely considered which we need to talk about.

For something to be considered a cash system, it is required to fulfill three main criteria. It needs to be a *store of value*, it needs to be a *unit of account*, and finally it needs to be a *medium of exchange*.

A good store of value is anything that can maintain its wealth without depreciating. Gold is a good store of value because it maintains its worth over time. Avocados are a horrible store of value because they can go bad fairly quickly.

If a nation-state's currency is a poor store of value, that would discourage people from using their currency. This would limit trade and it would generally compromise people's willingness to participate in the economy. To the right is an image of 1923 Germany, when the Republic of Weimar experienced hyperinflation. Wheelbarrows of cash were required to buy everyday items. Not good.

A proper unit of account makes sense of prices, costs, and profits. If your currency cannot be used to measure value,

then it is functionally worthless. How would anyone use it? That's like when you're playing with children and they're saying their toy is worth 2 doodads, but each doodad is worth 5 whatchamacallits, however each whatchamacallit can trade one-for-one for a toy. It's incoherent.

Lastly, a currency needs to be a medium of exchange. The currency is an agreed upon standard by all parties and it is used to facilitate trade of goods and services. We are likely very familiar with this in practice.

See that wasn't too bad. Now that we all have an understanding about what I mean when I say cash system (or currency), let's proceed.

What Is A Cryptocurrency?

Bitcoin is the first cryptocurrency. There is a complicated system of rules written by Jan Lansky that lists six different features of a cryptocurrency, but for the layman all you really need to know is it's a currency that is secured via cryptography. Simple.

The first thing we need to understand to get to the heart of what a cryptocurrency is would be cryptography (the "crypto" in cryptocurrency). You don't need to be able to "do" cryptography, but you should know what it is.

If you're like me, you might wonder what keeps your data safe in your computer, why you can't access other people's bank accounts, why other people can't access *your* bank account, etc. If you're not like me and don't wonder about these things, I'm going to tell you anyway (ha ha).

Cryptography is the practice of techniques to secure information. Let's pack up, time to go home.

Clearly there's more to it than that.

Have you ever sent a "secret message" to your friend in history class? Your teacher was babbling on about something boring that happened during the Byzantine Empire that you don't care about because Casey and Taraji are having a secret steamy romance their parents don't approve of. I can't say this happened to me because I was the nerd who actually paid attention in history class, but I believe that's happened to most of you to some degree or another.

In order to keep this message a secret, you decided to shift all the letters over by five because it makes the message look like garbled nonsense and the person will likely just throw it out if they run into it. This is cryptography, and that was called a Caesar Cipher. In the 21st century we have significantly more advanced methods of securing messages than that, but the fundamentals are still the same.

Let's say Alice and Bob want to send a message to one another, and they don't want a third party to read the message. Alice would "encode" the message-- or *plaintext*—with cryptography. There would be some rule the other person would have to follow in order to turn the jumbled alphabet soup—or *cipher*—back into a legible "plaintext" message. Still with me? That rule, is called the *algorithm*.

It wouldn't take a particularly intelligent person (especially if they're armed with a computer) to break the cryptographic scheme I used in my Caesar Cipher example. If you just *had* to know about the steamy romance between Casey and Taraji you could figure out what that message said. There are only 26 letters in the alphabet, and if you look at the message there's a very good chance that at least one of the words ends with the letter "s," or that there is a one letter word "I" or "a," that there are three letter words like "the," "and," or "for." With any one of those vulnerabilities you could try all 26 possible shifts of your letters and figure out what the common shift number is. If you are using a computer, you could just reprint the message 26 different times with each of the shifts...and you can do it in *less than a second*.

Out of necessity, we came up with more complicated ciphers. These usually involve a "key." In your day-to-day life, you should be familiar with this. The password to your email account is a "key," your ATM PIN, your fingerprint, etc. All of these are private keys. The assumption is, only

you or a trusted party are privy to the private key, and because of that, this can be used as your personal entry point to the secured information. Obviously, even this can create issues, but we will ignore those for now.

Back to Bitcoin.

Bitcoin uses modern cryptography to secure transactions.

Why Is It Called Bitcoin? Why Can't I Capitalize The C?

To bring it all together, the "bit" refers to the peer-to-peer portion and "coin" to the currency aspect. Bitcoin is a portmanteau (pretentious way of saying "compound word," makes you seem super cool, and every once in a while it'll win you a trivia game) of those two. You can't capitalize the "C" because it makes you look like you don't know what you're talking about. Lucky for you, at this point in the book you know more than at least 50% of people on the planet who exist at the time of me writing this.

As far as capitalizing the "B," there's a bit of contention. From what I can tell, you capitalize the B when you're referring to Bitcoin as an entity, and it's lowercase when you're talking about it as a currency--like US Dollars versus eight dollars.

Chapter 2

What Is A Blockchain?

Direct Answer: A decentralized online ledger that keeps record of all ‘transactions.’

Over the course of this chapter, we will cover the basics of blockchain and briefly touch on why I put transactions in quotations.

What’s The Big Deal?

Something that is rarely considered in our day-to-day financial life is the inability to spend money twice. We go to the store, and the store clerk asks us if we want to pay for our black licorice in cash or credit (oh, is that just me?), we choose our form of tender, the transaction is “approved” then we go about our business. If we are using *fiat* currency—currency that a government has declared to be legal tender, but is not backed by a physical commodity (e.g. dollar bills as opposed to silver shekels)--the act of handing the money to the other person acts as the

transaction, and double-spending is not possible due to you no longer having possession. In the case of credit/debit, while not tangible, the same process is occurring; however, it's your bank transfering the fiat currency from their reserves to the bank of the other person. In both cases, there is a physical transfer of wealth that occurs at some point which guards against double-spending. In fact, it's not even something you would consider (unless you're the kind of person that cheats at Monopoly by pocketing money you gave to another player).

In both of those scenarios, the transaction is guarded from double-spending either by the laws of physics, or by third-party validation. In this case, VISA or whatever other payment service you're using to secure the transaction, sends the data to your bank, who verifies the validity of the transaction and availability of funds. Your bank, who is in control of your monetary records, would transfer money from your account to the other party's. This transaction would now be added to both your account and their account.

All of this seems exceedingly obvious Tasheme, why have you spent a couple of hundred words on this? Great question.

In the cash example, the transaction happens without any form of verification. Sure, the shop owner could take out a counterfeit marker and double check the validity of the currency, but that is a "trustless" act. The shop owner can

rely on themselves and the quality of the tools available to them to determine whether the transaction is valid. In the credit/debit example, VISA, and potentially two banks need to be involved. They need to verify the transactions, update the *ledgers—the* record of transactions—associated with your accounts, then transfer the money as your proxy. This activity involves *trust.*

Here's the thing, trust can sometimes bite you.

Cash is king because cash works freely, and requires no third party verification. You feel secure in your transaction. That libertarian on your block who yells about the Fed and rising interest rates is perfectly okay with cash, but likely feels uneasy when it comes to credit/debit transactions.

The blockchain eliminates the need for third party verification.

Just like in the previous chapter where I explained peer-to-peer, the blockchain creates a peer-to-peer ledger of transactions, that all members of the system can verify—without trusting a third party. In effect, this turns your Bitcoin transaction into more of a cash or gold transaction. This is what is so revolutionary.

The Problem Of Double-Spending

I glossed over the double-spending problem above, but I think this is a very important aspect of Bitcoin. If you tire of technical details, you aren't losing too much by skipping this section.

Something that is unique to cryptocurrencies, is that it's made entirely of data. That means, after a transaction has been processed, one of the parties—or a separate one—can duplicate the coin, and spend twice as much. Given that it is digital, this counterfeited double spent coin, is indistinguishable from the original (This, is actually the problem of media/software piracy in a nutshell as well. Maybe there needs to be a blockchain for digital media?). To guard against this, the blockchain was invented.

The Bitcoin blockchain runs on what is known as a *"proof of work" algorithm.* All this means in essence is that there are a bunch of computers, *mining* coins. These miners use a ton of computing power to verify the validity of each *block*. Still with me? There's no one with a hat on, it's really not even a ton of people, usually it's a ton of computers in a really cold room.

Every time a transaction is made, it's added to a new block. At this point it is unverified. Now, this is where the

complicated comes in. Brace yourself. When it is added to the block, it is put through a *hash.* This is computer nerd speak for really complicated word scramble that is virtually impossible to undo. This word scramble is not random—if you put something in that's even slightly different you'll get a completely different result.

On each block, the transaction's hash is added to it. All of the miners then crunch numbers to determine if this chain of hashes is correct (i.e. this "block" - "chain"). If this chain is correct, then the block is verified and we keep it moving.

An attacker would target this process if they wanted to double spend. At that point, the hacker has to get a fake transaction onto the chain. This is exceedingly difficult. You have to get to the appropriate block, hash your transaction, put it in its appropriate position, while maintaining the integrity of all previous parts of the chain, and all of this has to be done before a new block gets made. If it does get made, you also have to change the new block, and so on and so forth. While theoretically possible, it is very **very** difficult.

In history, there have been several attempts to forge blockchains, or to send a fake copy to the seller, and a different copy to the rest of the blockchain. All of this has been met with very limited success. The easiest thing to do is to just take advantage of people not securing their information correctly, by stealing their coins.

What Is It Though, Is There A Big Computer Snake Somewhere?

The blockchain is really just a bunch of spreadsheets connected to one other. Seriously. Don't let any charlatans trick you out of your money because of their hocus pocus sleight of hand "once in a lifetime" investment trickery. It is just a system of connected computers that compares *chains*—record of verified transactions—to determine which is the longest. The longest chain is presumed to be the real chain.

While I am partially downplaying the blockchain's significance, it is done to highlight the lack of mystery involved in these technologies. Bitcoin isn't magic, it's "basic" computer algorithms your 20 year old son or best friend in college can perform. The blockchain is a natural consequence of other peer-to-peer networks that have dramatically changed the landscape of our world over the past couple of decades.

The revolutionary part is the creative implementation of these technologies combined with the economic incentive to propagate the system. The "once in a lifetime" opportunity present is your presence at the beginning of the blockchain revolution. The blockchain *itself* is not the

opportunity, but the consequences of a decentralized world.

Anyone can build a printing press (well most people, if you're given detailed instructions). When the printing press was created, though they were expensive, the true value was in how easily one could reproduce information. Eventually, presses were commonplace, but society was transformed.

But I digress.

Couldn't You Just Fake The Chain?

Yes. This would be called a 51% attack

Put simply, a 51% attack is when someone, let's call them the *adversary,* is attempting to create their own version of the chain. If the adversary owns 51% of the supply, then they would be exploiting the underlying mechanism used for consensus. They have the majority, thus their version of the chain is the correct one.

Having full control of the chain allows for the adversary to create new blocks given directly to them, it allows them forge transactions, or whatever else they can think of.

There have been a few successful 51% attacks. Most recent to the time of me writing this, Verge (XVG) had a successful 51% attack waged against them. The attacker had full control of the network for quite sometime and the coin has not recovered from the bad publicity since (This case is especially damning since the coin claims to be a “secure and private” coin). Lucky for Verge, most people don’t keep up with coin news during a bear market so they were able to retain a $450 million valuation.

Now, as I said before, pulling off a 51% attack is incredibly difficult. In fact, as time goes on, the likelihood that a 51% attack is even possible drops considerably.

For smaller altcoins like Verge, it’s possible because each coin has a relatively small value, and you simply need to patiently accumulate the circulating supply. When it comes to coins like Bitcoin, where over 80% of the supply is circulating, and each coin is worth thousands, plus there’s high liquidity, i.e. large number of buyers/sellers, it becomes exceedingly difficult to control over half the supply.

Additionally, changing upcoming blocks on the Bitcoin network could have catastrophic results, causing the price to crash which would negatively impact the value of the network. This of course would be against the attackers self interest, so it’s thought that coins such as Bitcoin might be resistant to this type of attack--though it is theoretically

possible.

Can A Blockchain Only Be Used To Track Financial Transactions?

In theory, it could be used to keep track of anything of value. The most obvious example I can think of would be identity verification.

If you want to get fantastical with me for a second, keep reading, but if you're more of a nuts and bolts, pragmatic type of thinker, the question has already been answered.

The purpose of the blockchain is to verify transactions without the need of a third-party. This, until now, has typically meant the verification of monetary transactions. Did you notice I had to use a qualifier? *Monetary* transactions. In theory, any transaction, monetary or otherwise can be used/verified on the blockchain.

This opens up a brand new world.

Seriously.

Think about the world prior to the internet. Things ran well, but it took far longer for information to travel. People had to rely on expensive long-distance phone calls to speak to

people around the planet. Everything was separate.

The internet allowed for people and things to be connected. It created networks, and as the internet has matured, it has permeated all aspects of our lives. The divide between online and offline has dissolved; for better or for worse.

Technological and social networks are at the core of our society now and, currently, they are ran based on attention. Attention is the backing to our network economy. You have value on YouTube if you have viewers. You have value on Instagram if you have millions of followers and tons of "likes."

Initially, these likes and follows had power, but more of an abstract type of power. People would mobilize their follower-base to perform different tasks--like boycott--but that's all they could do. In the present, companies have been able to monetize and leverage this power by paying social influencers to advertise their products, but that's kind of like the old paradigm trying to stay relevant.

Blockchain is the first step into the new internet paradigm.

That sounded a lot more "buzzword" than I would have hoped, but it's true.

With decentralized verification of transactions, your instagram like can and *will* have true economic power. Each like can award cryptocurrency.

But let's step outside of money itself. How else can this be applied?

Think about contracts. As of now, you need a lawyer or a notary to substantiate the contract. With the blockchain, you no longer need that. A smart contract can be drawn up, and if you violate the conditions of the contract, the consequence will execute. Additionally, because there is no third-party, just cryptographically secure computer code, the contract will execute its conditions *no matter what*.

Let's get a little bit kooky, and let's think about the future of autonomous cars. As of right now, we have drivers. You call an Uber, and your driver arrives, you pay the driver, and voila, you're off to your location. When cars become autonomous (which we already have the technology for), your car can be set to "ride share" and it will go around picking up people and taking them to their destination--without you present. Who will make sure your money gets to you, since it is your car after all? Well, your car will.

Let's take this one step further. Community-owned cars. We get to the point where it's *inconvenient* to own your own car. You live in the City and parking is limited? Well, your City has autonomous cars that drive around, and operate themselves. They initiate transactions **for themselves,** then voila!

There are potentially unlimited applications that exist, but we're in the infancy of the blockchain so it's easy to be myopic.

The blockchain further entangles the internet with the real world.

Chapter 3

How Can Something Be A Currency If It's Not Physical?

Direct Answer: supply and demand

This is a question I commonly come up against, and I believe this gets down to the crux of what Bitcoin really is.

To give you a good answer to this question, I have to take the scenic root and explain to you the *other* reason Bitcoin was created in the first place. On the one hand, Bitcoin was created in order to remove the middle-man and allow for trustless transactions without the need for any corporation or government. On the other hand, Bitcoin was created as a response to fiat currency.

The founder(s) of Bitcoin, Satoshi Nakamoto, decided to create Bitcoin because he felt the central banks could not be trusted to not debase the currency. Here's a direct quote:

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.*
>
> -Satoshi Nakamoto (Bitcoin Open Source Implementation Of P2P Currency)

Pretty cut and dry.

As a response, he chose to make a trustless *deflationary currency*. We've covered, the trustless part, but let's dive into what makes something a deflationary currency.

What Makes Something A Currency?

As we said before, for something to be a currency, it needs to satisfy a few key criteria. It has to be a *store of value*, be a *unit of account*, and a *medium of exchange*. Additionally, there are several functional definitions it need to abide by to be a useful currency. Those being:

1. Durability
2. Portability
3. Divisibility
4. Uniformity

5. Limited Supply
6. Acceptability

We are pretty familiar with the first few criteria. Money has no purpose if it's not a store of value. Due to it having value, it as a consequence becomes a "unit of account." It serves as a meter for the value of economic transactions. Pretty straightforward. Lastly, since it "stores value" and can be used to account for the worth of an economic exchange it, as another consequence, can be exchanged for goods or services. The money is inherently valuable, it has a defined value, and as a consequence it can be given to another as a medium of exchange.

The other criteria are where Bitcoin and other cryptocurrencies show their true value. They are durable because they're simply digital signals that traverse the internet. They are exponentially more portable than fiat currency is. In fact, they don't need to be carried *at all.* Most cryptocurrencies are divisible. Bitcoin in particular can be divided infinitely, but is traditionally divided up to 8 decimal places. Each unit is referred to as 1 **satoshi**--in honor of the Bitcoin creator. Every Bitcoin is the same as any other, so it is entirely uniform. There will only ever by 21 million Bitcoin in existence, so it has a severely limited supply. Lastly, it is accepted globally. Bitcoin has no borders.

In essence, Bitcoin in particular, but cryptocurrencies more generally, are more efficient than standard currencies.

Okay, I Get That. Where Does The Deflation Come In?

The US Dollar, and most forms of currency you may be familiar with, are inflationary currencies. There are a couple of agreed upon reasons for inflation, but the gist behind inflation is simply that, over time, the supply of the currency increases and consequently the price of everything increases as well. This is due to the fact that no individual amount of currency is as valuable as it had previously been.

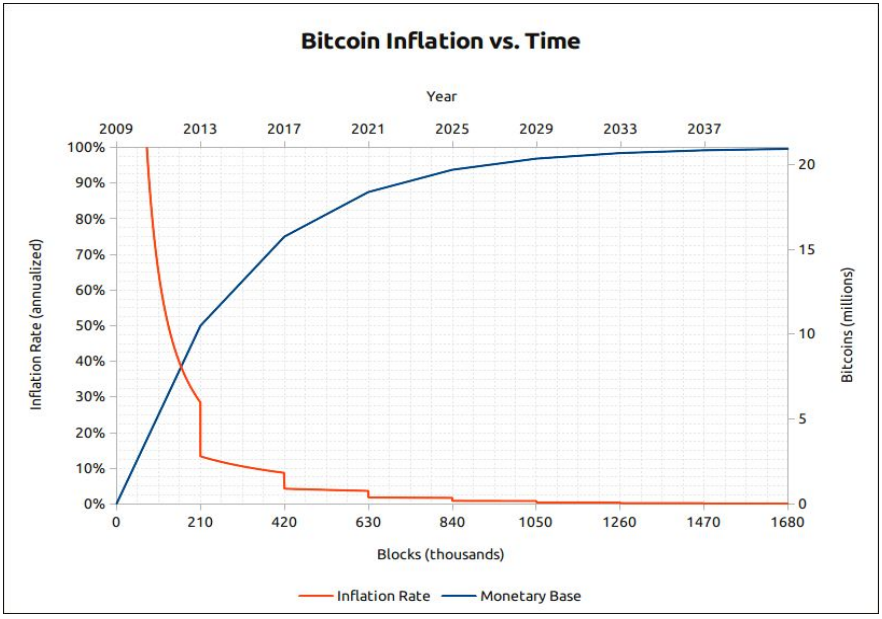
Essentially, we've diluted the value of each individual denomination of currency.

The part that was truly reprehensible to Satoshi was that the central banks are the ones that increase the currency supply. Someone at the Federal Reserve, does some calculations, and they determine how much more money needs to be printed in order for all of the math to "balance itself out."

After the Financial Crisis of 2008, our collective trust in the system dissipated, and Satoshi began creating Bitcoin.

Deflation is the opposite of inflation.

The supply of the currency is limited and as a consequence, each coin retains its value. In fact, as the currency is used more, the value of each denomination of the currency increases. Every time someone loses a denomination of that currency, the value of the remaining currency increases. For holders of the currency, everything begins to get cheaper.



Source: bitcointalk.org, user: whitslack

How Can You Just, “Print Money?”

This is what frustrates people.

There are several mechanisms that allow for central banks to simply “print money,” but the most crucial of which is called *fractional reserve* banking.

When you give your money to your bank, they do not just house the money safely inside the bank and all is hunky dory. The bank would never make any money this way. What happens instead is, the bank keeps a *fraction* of the money that you have deposited in its *reserves.* The rest of the money is loaned out to people for interest. The bank then collects revenue from the interest from these loans.

An interesting consequence of fractional reserve banking is that there is now more money in circulation than should otherwise exist.

If you put $100 into the bank and the bank decides to retain 10% of that $100 — or $10, then they are now free to lend $90. On paper, that puts $190 in circulation despite there only being a *true* $100 in existence. The remaining $90, though treated as real money, has in fact zero real added value, all that has happened is the overall value of each denomination of currency has gone down.

Sketchy, huh?

Note: There are some economic and mathematically sound reasons that could be used to validate the use of fractional reserve banking, but it is important that you understand Bitcoin's underlying ethos.

What Happens To Your Money If Everyone Withdraws All Of Their Money At Once?

Welp, you get the 2008 Financial Crisis.

The banks obviously don't have that money, so the banks insure up to $250,000 of your dollars with the FDIC or some other regulatory company. Even with that, in major financial crises, there isn't enough money to go around. Typically, the government--understanding how fragile the system is--will often bail the banks out in order to prevent financial collapse.

Okay But, Again, How Can It Be A Currency, If It's Not Physical?

In the modern era, you likely work with digitized currency in your day-to-day life far more than with anything else. You

likely swipe your debit or credit card or use some other digitized payment service more often than not.

Prior to the modern era, we used bills or monetary notes to act in proxy of precious metals. The coins were far too heavy, so it simply became more efficient to use bank notes. The notes have a denomination on them, and they act as legal tender in place of explicitly transferring gold or silver--which were quite cumbersome.

Somewhere along the line, many governments actually have detached the notes from their physical backing. Remember our conversation about “fiat currency?”

What’s funny is, when you swipe your debit card, you’re dealing with an abstraction *of an abstraction* of value. You can probably see why Satoshi--and many others--are a bit skeptical.

Bitcoin is backed by energy expenditure. If you have veritable proof that digital work had occurred, you can exploit the underpinnings of capital--which places monetary value on labor, and grant each coin the intrinsic value of that work. If you don’t view that as concrete enough, the limited nature of energy, and the work done to generate and use it, acts as another more tangible financial backing.

Where Can I Use Bitcoin?

At the moment, this is one of Bitcoin's pitfalls. Satoshi envisioned Bitcoin to be a peer-to-peer cash system, and yet, I can't use Bitcoin at the grocery store--at least not in most countries.

There are two major schools of thought when it comes to the path that Bitcoin will take towards mainstream acceptance. The first path, is for Bitcoin to follow the standard technological adoption curve. Where we stand right now, Bitcoin is a relatively new technology and it's lack of acceptability is mainly due to the hesitancy that masses of people have towards adopting new technologies. This camp believes that once it's convenient for businesses and consumers to implement Bitcoin transactions, then they will do so. There are a few ways that this can occur. The method that is briefly outlined in the bitcoin whitepaper would be after Bitcoin's price has inflated, then transferring wealth on the blockchain would function like the transfer of wealth in any other form. The volatility we experience moving from a value of 5,000 USD to 6,000 USD is an increase in 20%. This type of move is monumental and would completely disrupt businesses. However, the move from 1,000,000 USD to 1,001,000 USD is only 1%. This is the sort of move we experience in our fiat currencies, and we hardly notice.

The second, and more controversial camp, is called *hyperbitcoinization*. Essentially, as the US Dollar--or substitute your fiat currency of choice--collapses, Bitcoin's value will be seen. When this occurs, Bitcoin will become the global currency, and its necessity will fuel it's global adoption. At this point, each satoshi will be worth about as much as 1 USD and we will begin our transition into a global society. Depending on when you read this, their claim will either be hilarious or the obvious course of history.

Chapter 4

Which Bitcoin Is The Real Bitcoin?

Direct Answer: It's complicated. I truthfully can't give you a direct answer.

There are quite a few cryptocurrencies out there that share the Bitcoin moniker. Whether it's Bitcoin Dark, Bitcoin Gold, Bitcoin God, or most notably Bitcoin Cash. It can become easy to get lost in the myriad of Bitcoin-like coins. Which of these is the real Bitcoin?

For the most part, you can cross most Bitcoin-like coins off of the list if they were made prior to August 1st, 2017. It's very unlikely that even the coins themselves would argue much with you. However, there is a very heated debate in the cryptosphere about the validity of two coins in particular: Bitcoin and Bitcoin Cash.

I have done my best to be as straightforward with you as possible, and I'm going to let you know right now, that this is easily going to be the most controversial chapter of this entire book.

The community has been divided on this issue for quite some time, and it is probably the most emotionally laden topic in the entire space. I am going to try and provide some insight on the matter, but before anything I need to explain a few things.

Bitcoin Is Open Source And Decentralized

Several attempts have been made prior to Bitcoin to create an e-currency. None of them worked. Satoshi believed that it was due to the centralized nature of these currencies.

"Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own."

-Satoshi Nakamoto

(Re: Bitcoin P2P e-cash paper)

It would make sense. He's creating a currency that would effectively undermine the dominance of national currencies. It's important for the currency to not be silenced otherwise it would not be able to grow.

In order to properly implement this protocol, he also made the Bitcoin code open source. Anyone could participate in the creation of Bitcoin. Anyone can run Bitcoin. By making Bitcoin open source, it is truly decentralized, and thus it is unstoppable

...however, by making Bitcoin an open source project, you also make it vulnerable to *forks*.

What Is A Fork?

In any open source project, developers need to be able to add to the existing project; however, if every developer started writing on the master, then the project would be chaos and it wouldn't get very far. In order to rectify this, developers can "fork" the repository. The forked version then splits off from the original version, like a fork in the road.

Typically speaking, the developer would then update the code on his version, and "push" updates onto the original version. This process would then merge the two separate forks into one program. However, there are cases when the new version and the old version are incompatible, and as a consequence the two projects split off from one another and go in two different directions.

With Bitcoin, there have been many forks, most of which have been *soft forks*.

A soft fork is usually some update to the protocol and previously valid blocks are now made invalid. This change

is backwards compatible, i.e. older nodes can implement this change without having to upgrade.

This decision regarding soft forks are left up to the community, and when a majority of the nodes agree, they fork is implemented. Remember, if the majority of the nodes want to go in a different direction, they have control over the “longest chain.”

Below is a diagram about how a soft fork works.

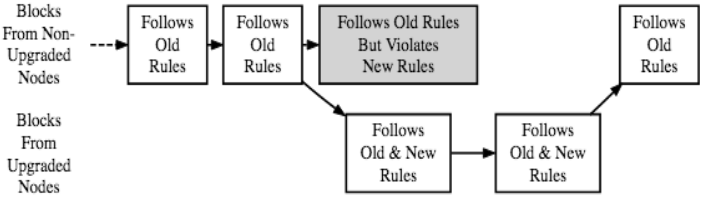


Image: Investopedia

Moving from left-to-right, the chain exists with non-updated nodes. These nodes follow the “old rules” of the system. That is, they are operating prior to any change. After the second block, a soft fork has been implemented. The shaded box are those nodes that were previously valid, but now violate the new rule(s) that has been added to the system.

As a consequence, those nodes are no longer a part of the "longest chain." They are now obsolete or invalid.

Below the invalid nodes are those nodes that satisfy the old and new rules. No upgrade was necessary, they are simply the next link in the chain. The nodes now continue on as if nothing happened, connecting to the next valid node.

To avoid confusion, the furthest block to the right labelled "old rules" refers to all rules prior to itself. From the perspective of that block, the new upgrade is considered an "old rule."

In contrast, there exists what is known as a *hard fork* (I bet you didn't see that coming).

Hard forks are quite different, and they are usually due to a fundamental disagreement about the direction a coin ought to take. The most notable hard fork is Bitcoin Cash--trust me, I will talk about this soon.

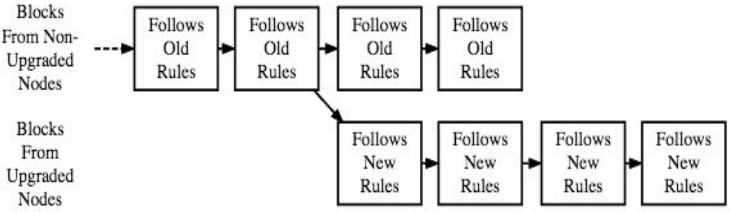
Essentially, the community decides to implement a new change that will fundamentally alter all blocks that will exist going forward. If all members of the community agree, then great, no issues, and the old fork simply dies. However, since we are human, we can rarely agree on anything.

If there is a lack of consensus, then at a specified block, the codebase splits, one of which implements the new rules, and

the other implements the old rules. This leaves you with two separate coins that have a *shared* history.

Typically, the holders of the coin pre-hard fork are rewarded with both coins in what is called a *1:1 airdrop*. A nice reward to the community for holding through the ruckus, but also as a means to create free promotion for the new coin. What works better for a promotion than free money?

Below is a diagram that illustrates a hard fork.



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Image: Investopedia

As in the last diagram, the coin has a singular shared blockchain until we reach the third node where the codebase forks. Now, you have two separate coins, with two distinct blockchains. It is important to note that this type of fork is *not* backwards compatible. The two chains are diverging and creating two separate entities that will only become more and more dissimilar over time.

Bitcoin Cash And The Segwit Debacle

Alright, now I've brought us to the most contentious issue in the cryptosphere. I will first provide a brief background on the issue, then I will present both sides of the debacle, and finally I will provide my opinion. I want to make this **abundantly clear**, I have not been paid by any party. I have no affiliation with any party. I am simply a member of the crypto community that doesn't feel any strong ties either way, and I feel like I can pretty objectively speak on the matter given my expertise in the space.

Now that the disclaimer is over, let's get down to it.

SegWit

To begin, Bitcoin was beginning to experience "congestion." The developers as well as many in the community noticed that this would become a major problem as time went on. If the blocks are overly congested, it will take a long time for transactions to be confirmed on the blockchain, and the dream of Bitcoin competing with payment systems such as VISA would be over.

Great, the community identified the problem, now they just had to agree on a solution.

Two solutions were proposed. *Bitcoin Unlimited* and *SegWit.*

Bitcoin Unlimited's idea was simple. Completely remove the block size limitation on Bitcoin. The purpose of the 1MB limit on each block was simply to guard against DDoS attacks--or *denial of service attacks* (it's really not important to have a strong grasp on what that means, just know it's annoying hackers filling the blocks with junk).

The miners loved this idea. From their perspective it was great, if you have no cap on how large blocks can be, then it will require that much more effort to mine each block and consequently, each block rewards the miners more. Perfect!

However, the community figured that this would centralize mining. If blocks get too large, then only the largest mining pools--or groups of miners--could mine blocks; the little guy would be completely SoL.

Ultimately, the community shied away from this idea.

The other proposal was SegWit. Short for "Segregated Witness," the developers figured they could kill two birds with one stone. In every Bitcoin transaction, there's a cryptographic signature that essentially validates the transaction; however, up until this point, the signature did not contain all of the data about the transaction, so it was theoretically possible to alter the signature in such a way that you can sneak extra Bitcoin into the transaction. This is known as *transaction malleability*.

The developers, using some serious programming voodoo, decided to frankenstein the transaction process, “segregating” part of the transaction information, and taking it off the blockchain. This would allow for them to put more transactions into each block--since a piece of the transaction data has been removed--and this new feature can be exploited to solve the malleability problem.

Though this solution ended up being implemented, many people thought this was simply a temporary solution to the problem, and that the Bitcoin Unlimited approach was better.

In order to satisfy everyone, a compromise was made. This protocol, named SegWit2x, both stored some of the transaction data outside of the blockchain, and increased the block size to 2MB. Ultimately, 95% of miners agreed to the proposal, and the changed was implemented.

...here is where the controversy begins.

Bitcoin Cash

Some people were not too keen on this SegWit2x proposal. Many prominent figures in the cryptosphere were very vocal about their opposition.

You see, the issue they had was...well, at the risk of sounding like a meme, that SegWit2x went against "Satoshi's true vision."

Limiting the block size will eventually create congestion in the Bitcoin network. Ultimately, the price for transactions will increase to such a point that micropayments will be infeasible. The idea that you could go to the store and buy a $3 coffee would be completely off the table.

Thus, at the Future of Bitcoin Conference, a developer by the name of Amaury Séchet proposed Bitcoin ABC, the first version of what would later be known as Bitcoin Cash.

Sechet and his team of developers decided to increase the block size limit to 8MB, which is such a drastic change from the Bitcoin protocol that a hard fork was required. Additionally, the team made it clear they had no real aversion to increasing the blocks further down the road. To them, the block size was simply a means to an end. If Bitcoin cannot be used as a means of exchange due to block congestion, you can indefinitely increase block size. Eventually, computing power will match.

Due to its consistently low transaction fees and general business focused philosophy, Bitcoin Cash was an immediate success. Within its first day of existence, it jumped to the third largest market cap.

“Bitcoin’s usefulness as a store of value comes as a secondary effect from its usefulness as a medium of exchange. If you destroy the medium of exchange, you destroy the store of value.”

-Roger K. Ver CEO of Bitcoin.com

Bitcoin Cash gets a lot of hate.

The Bitcoin community believes that it simply is profiting off of the Bitcoin moniker and that many of its marketing techniques are being used to deceive newcomers. For instance, Bitcoin.com is owned by Roger Ver, who is one of the largest Bitcoin Cash supporters. Since Bitcoin.com is ultimately about Bitcoin Cash (henceforth referred to as BCH), many believe that it is clearly fraudulent enterprise aiming to deceive.

In response, Roger Ver as well as Jihan Wu have argued by saying that “Bitcoin Cash IS the real Bitcoin.”

Pause.

We have had the opportunity to speak about the essence of Bitcoin. We have talked about the Bitcoin whitepaper and we have talked about forks. Let’s take a moment to rationally analyze this situation before we continue.

Bitcoin Cash is the byproduct of a hard fork.

That's it, we can wrap up here. BCH is clearly not the original. Look it even has a different name!

Well, not quite.

Let's think about the origin of BCH. The community decided to implement a change. S2x was designed to change the Bitcoin protocol. It was a hard fork in itself. Let me repeat. S2x was a hard fork from the old Bitcoin protocol.

We have seen the chart. That means there are now two separate blockchains, but prior to the hard fork, the two chains have the exact same history.

Well, here's where the funny business starts.

Technically speaking, BCH implemented its hard fork on August 1st, 2017. That means up until August 1st, 2017, BCH and BTC had the exact same chain. They were the same entity. Let's call the pre-hardfork chain, **chain A.**

Now, when BCH created its split, BCH became a spinoff of **chain A.** This spinoff has one difference, instead of having a cap of 1MB on the blocks, BCH has a cap of 8MB. As far as changes are concerned, it's significant, but in practice, the coin is effectively the same. The blocks are too large to be filled easily, so BCH operates pretty much identical to **chain A.**

In fact, if we double back to the section on SegWit, BCH is much like the Bitcoin Unlimited proposed solution.

Okay, so now on August 24th, the standard Segwit soft fork occurred, thus old nodes that did not follow the new rules were invalidated, and the chain continues on with the backwards compatible update. This new post SegWit chain is now going to be called **chain B.** It is fundamentally different from the original **chain A.** Bitcoin acts differently after this implementation. If you remember, SegWit changes the way in which transactions are implemented and stored in the block. There is a far larger change occurring here than with the BCH fork.

Finally, off of **chain B,** there is another hardfork that occurs. This being S2x. **Chain B** still exists, and BTC--with the S2x implementation, forks from that chain into a third chain.

Which is the real Bitcoin?

Now we're dealing with a pretty interesting philosophical question.

Note: I can't resist the urge to wax poetic for a second, if you're not interested in the thought experiment feel free to skip this next section.

Ship Of Theseus

The way this goes is the great hero Theseus has a ship that he sailed on to battle. During his adventures, boards would rot from the sea water and were replaced. Each time one of the boards were removed, they were brought back to his home city and assembled in a museum. Eventually, all of the boards in Theseus' ship were replaced and in the museum stood a perfect replica of Theseus' original ship.

Which is the real ship? Is it the ship made entirely from new boards, or is it the ship in the library made entirely of the original boards, then reassembled?

Is there a metaphysical--or, some would say, spiritual--property present within the object? Does the essence of the ship carry on to its new form? Is this new ship--completely different in every respect--the same ship? The "natural" inclination we have is to say "yes!" We have quite a lot of experience in this regard. The cells in our body are replaced every 7 years or so, we are effectively a completely different entity, but there's a lasting continuity. Many cultures refer to this as a "soul." Secular cultures would refer to this as an "ego."

On the other hand, a ship has no "essence." Its existence is physical, it is a tool comprised of specific parts in a

specific arrangement. The real ship is the recreated ship in the museum. All of the pieces are identical to the original ship. All of the pieces are in their appropriate place. It's clear that the essence of a thing is simply an illusion, and the actual entity is the parts it is comprised of. We have difficulty not viewing the recreated ship as being the original due to our predisposition towards object permanence.

I am sure you have your opinion, but there's really no correct answer on the matter.

Back To Bitcoin Cash v. Bitcoin

Who has the real coin?

Technically speaking, Roger Ver's claim that BCH is the real Bitcoin is really not that far off. BCH is much like the ship in the museum. It is closest to the original BTC protocol. Functionally speaking, it operates in the same way as the Bitcoin that existed prior to SegWit, like the Bitcoin that experienced the parabolic runup. Are his marketing strategies a bit unethical? Probably. But in a hyper-capitalistic, unregulated, dog-eat-dog market, that's what you should expect.

Bitcoin--or Bitcoin Core, if you're a BCH fan--is the current iteration of the chain. It is *also* Bitcoin. It is the ship that Theseus continued to sail on; the ship that had to replace its rotting boards. For all intents and purposes it is actually the true Bitcoin because it has continued on with the metaphysical essence of the original Bitcoin.

If you're of the opinion that BTC is the true and only Bitcoin, you're incorrect philosophically speaking, but functionally, you are correct as well.

I told you these things can be tricky.

You as the reader are free to make up your mind on the matter. I don't care either way.

For the sake of transparency however, I will elaborate on my opinion briefly.

My Take On BCH vs. BTC

Due to the direction the current version of the Bitcoin protocol is taking--S2x and it's adoption of the Lightning Network (discussed in the next chapter) --I think that is has begun to shy away from its original idea of being a decentralized P2P electronic cash system. I believe Lightning Network--while being a very clever programming

feat--serves to centralize the Bitcoin network, and makes it a lot more like VISA than a decentralized cryptocurrency.

For that reason, despite it being the metaphysical continuation of Bitcoin, it is way different than the original essence. Is this a bad thing? Not really, I actually am curious to see how the experiment plays out. There's a level of intelligence found in the crowd, especially in the case of open source projects. This could turn out to be a great direction for the coin, especially since the Lightning Network does open up room for smart contracts. However, it is pretty impossible to argue that Bitcoin Cash is not Bitcoin. It has a shared history and it is closest to the original protocol. Just saying.

Chapter 5

What Is The Lightning Network?

Direct Answer: A method of conducting Bitcoin transactions off of the blockchain in order to decrease congestion.

As we spoke about in the last chapter, the popularity of Bitcoin, and cryptocurrencies in general, experienced a meteoric rise over the past several years. While the original intent has always been for large scale mass adoption, practically speaking, there have been a few technological hiccups.

The scaling issues that Bitcoin experiences has had two proposed solutions. The first being simply to remove the cap on block size, allowing more transactions to fit on each block. The second solution was to change the way transactions occurred. The idea was to change what information was stored on the block and to conduct the rest of the transaction *off-chain.*

These two solutions caused the community to splinter, and about 95% of the community decided on the second solution. This path was known as SegWit, and the ultimate goal of SegWit was **The Lightning Network.**

How Does It Work?

LN (henceforth how I will refer to The Lightning Network) is often misunderstood, and quite frankly for good reason. It is a conceptually and technologically difficult protocol to understand.

Lucky for you, you have this book, and you will officially be more well informed than your peers.

Fundamentally, LN relies upon the idea: “If a tree falls in the forest, and no one is around to hear it, did it happen?”

...I’m seriously not making that up. It’s in the official whitepaper.

Essentially, the creators of LN, Joseph Poon and Thaddeus Dryja, foresaw the scalability issues that BTC would experience. Comparing BTC to the VISA network, Poon and Dryja noted the astronomically large block size that would be required to handle a similar load. While Moore’s Law may indicate the possibility of this working in the future, they felt it important to mitigate this issue in the present.

“The payment network Visa achieved 47,000 peak transactions per second (tps) on its network during the 2013 holidays, and currently averages hundreds of millions per day. Currently, Bitcoin supports less than 7 transactions per second with a 1 megabyte block limit. If we use an average of 300 bytes per Bitcoin transaction and assumed unlimited block sizes, an equivalent capacity to peak Visa transaction volume of 47,000/tps would be nearly 8 gigabytes per Bitcoin block, every ten minutes on average. Continuously, that would be over 400 terabytes of data per year.”

-Poon and Dryja (The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments)

The above quote is a bunch of technical jargon that amounts to: “we’re going to need a bigger boat.”

Effectively, LN opens up a private payment channel. Both parties, agree to open this channel and put up a specified amount of BTC each. Once the channel has been opened, the two parties are free to exchange with one another as often as they like. The initial wagered BTC that opened the channel acts as their consent to exchange. These channels are what we call *smart contracts.*

Once both parties agree to either end their payment channel or if either party disagrees with the nature of a transaction, the channel will close, and the final net balance will be posted on the blockchain. In the case of

a disputed transaction, the final mutually agreed upon balance would be posted to the blockchain. All of the transactions prior to the final ending balance are deleted along with the payment channel, and the last successful transaction is posted on the blockchain in the form of the final ending balance.

LN would effectively act as a connection of indefinite payment channels. Limiting the posting of transactions simply to the final ending balance, drastically reduces the amount of data needed to be stored, and consequently allows for the network to scale.

In effect, all of the transactions that occurred within the smart contract, never occurred as far as the blockchain is concerned because “...no one was around to hear it.”

Is This Safe?

In the previous chapter, we briefly touched on transaction malleability. The theoretical weakness found in Bitcoin transactions would make LN incredibly insecure. Since a secondary payment channel is being opened, if an adversary were to alter the outcome of the final transaction, the payment channel has already closed, and the other party couldn’t do much about it. This is why the push for SegWit was required.

There is another security limitation however. In order for the dispute feature to work, it would theoretically require all users to monitor the blockchain for fraud. This of course would never happen. As a response, they created “watchtower” nodes.

Here’s the thing.

If you’re entrusting “watchtower” nodes with the power to settle disputes, you’ve now just created a trusted third-party. If you remember, the whole point of Bitcoin is to be a trustless peer-to-peer cash system.

One could argue that this isn’t quite the same as having a trusted third party because the nodes are within the Bitcoin network, and you would have a point.

Who knows? This is one of those situations where only time will tell if this was a good decision for the protocol or not.

Chapter 6

Is This Even Legal?

Direct Answer: Yes, but not all of it and not everywhere.

As it currently stands, Bitcoin has not been made illegal anywhere. Which, for all intents and purposes, makes it legal. The issue is, it is such a new technology, that allows for so many things to occur, that there exists a lot of potential to break the laws of your country or another country. Bitcoin is decentralized and global; which country's laws does it abide by? Are you breaking the law by using it?

It makes perfect sense to be confused about the legality of Bitcoin because quite frankly no one is 100% sure about how Bitcoin and other cryptocurrencies should be handled under the law.

At the same time, Satoshi, as well as diehard BTC users feel as if it is above the law. That the entire point of creating this trustless decentralized system was to circumvent the short-sided nature of nationstates and government. It was to free the people to commerce with

one another and govern themselves. These people feel that no bank, government, or person can or should be able to have centralized authority over the network, and that it should be “for the people and by the people.”

Is Bitcoin Useful For Illegal Activities?

Yes.

I bet you expected me to spin the issue.

Yes, Bitcoin is used for illegal activities, but so is cash. In fact, cash is anonymous and you can spend it on anything. You can buy drugs or prostitutes in the United States (where I am writing this book), but they are both illegal. By the same token, Bitcoin does allow for users to circumvent local laws and participate in illegal activities.

Hopefully, by now you’re beginning to see that Bitcoin and other cryptocurrencies are so much more than that.

Is Bitcoin Anonymous?

This is such a common misconception, and it's important that, as a user you understand, unequivocally, that **Bitcoin is not anonymous**. In fact, as we already know, all transactions are posted on the blockchain. Bitcoin is *extremely* transparent.

With that being said, there are projects such as Bitcoin Private (BTCP) or Monero (XMR) that claim anonymity (BTCP is a hardfork from the Z Classic coin). I am not familiar enough with many of these coins to speak on them, but it is important that you understand the distinction.

Now, there is a level of anonymity that this hypervisibility provides. When you have millions of transactions, all of which are associated with different hex strings that we use for our wallet addresses, it does allow for a user to be lost in the noise. Plus, you are always free to create new Bitcoin wallets, hide the private keys and make sure that no association exists between you and the wallet. This is not anonymity though. There is nothing stopping an entity from tracing all of your transactions through the blockchain.

It has been said, "bItcoin is about as anonymous as a prank phone call."

Take from that what you will.

Can Bitcoin Be Regulated?

Like many other questions I have attempted to answer for you, this one is tricky. There is a lot that makes Bitcoin incredibly resistant to regulation, but with a little bit of creativity, governments can impose indirect regulation.

First and foremost, no one can gain access to your Bitcoin if you store it in a Bitcoin wallet and you secure your private keys. Now, it's possible that third party wallets can be hacked, but as far as we know currently, the wallets themselves are pretty failsafe. It is possible that computing power can advance to such a point that the wallets are no longer safe, but if that occurs, there will be much bigger problems to worry about. Your standard bank accounts and pretty much all private records in most institutions would be at risk as well.

If your Bitcoin is in a trusted Bitcoin wallet, no government can reach them.

Great! But, not really.

How do you buy the Bitcoin? Typically, you need to go through an exchange. These exchanges are businesses and they are registered with regulatory government business bureaus.

Okay, let's say you're not interested in buying Bitcoin, and you'd rather mine it instead. Well, now you're putting out spiked electricity usage, and unless you're clever enough to hide it, your power company can likely figure out what you're up to. That power company is under government regulation.

Let's say you already have Bitcoin and its in a wallet, and you don't plan to buy from any exchanges that have any chance of being audited for whatever reason. How do you cash out?

This problem gets really tricky. Unless there's some massive overhaul to the global financial system (very possible and could happen sooner than we think), there are a lot of complications at play.

However, I can say, as long as you're using Bitcoin and running Bitcoin transactions to and from other Bitcoin wallets, it would be incredibly difficult for a government entity to do anything about it.

What About Taxes? Do You Have To Pay Taxes On It?

Refer to the above. If you cash out your Bitcoin, and all transactions are on the blockchain, if the government

entity knows of your wallets, they could trace your coin and theoretically take you on capital gains, amongst other things. This would primarily be an issue if you were cash out on an exchange of some kind.

Additionally, if you're trading bitcoin on an exchange that has asked you for your personal details, such as a passport or social security number, they are likely trying to stay in good graces with the IRS and SEC, in which case the exchange can and will gladly hand over your tax information.

It is also theoretically possible (but highly unlikely given how slow the tech adoption curve is for government agencies) that they could run AI to track your Bitcoin through the blockchain, and they could then pretty easily tax you as well. This is more hypothetical, very unlikely.

Is The Consumer Protected?

This depends on what you mean by protected.

In a cryptographic sense, yes. The consumer can participate in trustless transactions with other entities and know that their exchange will go through as planned.

However, if your oldest son is going off to college and you wanted to send him tuition money, but you accidentally made a typo in his wallet address, now thousands of dollars are lost in the ether, are you protected? Will you be reimbursed?

No.

This is both the blessing of crypto, and what I believe will hold it back from mass adoption at the moment. This "feature" is a consequence of the libertarian principles that underlie the technology.

The creators were big on personal freedom and subsequently personal responsibility. Because of this, you now have to assume responsibility for lost coins. Similarly, if you forget the private key to your Bitcoin wallet or if you are the victim of theft, you are completely responsible.

There is no central authority, and thus there is no one you can go to in the event of an accident.

There's a possibility that crypto insurance becomes a thing (a few companies already exist from what I've been told), or that some other third-party finds a way to rectify this issue, but that's how it stands at the current moment, for better or for worse.

Chapter 7

Alright, I’m Sold. How Do I Get Some?

Direct Answer: Either buy on exchanges or mine.

Here we are at last. You have learned about all of the underpinnings in Bitcoin and the basics of the cryptosphere. You’re sold, you want some Bitcoin, but how do you get it?

We’ve spoken about some of these methods briefly, but this chapter will cover them more extensively. It will also briefly mention things you ought to look out for in the space.

Note: All of this information is as it stands in 2018 and it’s very likely that this information could becoming outdated in the future.

Mining Bitcoin

As a disclaimer, this is not my forte. There are many amazing books and resources available on Bitcoin mining, but I will let this section serve as a primer.

Earlier on, we spoke about what mining is, so how do you get started?

First, you're going to need a PC with a strong graphics card.

In the early days of Bitcoin, the mining difficulty was set to be far lower, so there was a far lower barrier for entry. At this current moment, unless you have several particularly strong PCs with a very strong graphics cards, it will be extremely difficult for you to mine.

Additionally, since Bitcoin is a proof-of-work coin, the value of each coin comes from the energy expenditure. Since I am not psychic, I do not know how expensive it is to mine Bitcoin at the time of you reading this, but at the time of me writing this, Bitcoin is hovering around $6,000 USD and it costs roughly $8,000 in the United States to mine. At the time of my writing this, it costs around $25,000 to mine in South Korea. This clearly won't do.

If you live in another country, or have connections, you can mine profitably, but unless you live somewhere like Trinidad & Tobago or Venezuela, you're likely out of luck--if you're an individual (the cost to mine BTC in Venezuela is currently $500 per coin).

If things change between the time of me writing this, and whenever you end up reading this, then this is what you do:

First, you would install a miner. With a standard PC this should be pretty straight forward. Once the miner is installed, you set it up, and let your graphics card run. Easy peasy.

Buying Bitcoin On Exchanges

There are quite a few exchanges, and every year more are added to the list. Depending on your country of origin, you could be using one of a myriad of exchanges. As an American I will provide an American's viewpoint, but there are currently, and there will be many more, exchanges that allow for Bitcoin buying in EUR, JPY, KRW, etc.

When you're choosing which exchange to buy your Bitcoin from, it is very important that you determine whether you're buying "shares" of Bitcoin or if you're buying actual Bitcoin that will allow for you to withdraw and store the private keys.

At the current point in time, exchanges like Robinhood, have their own store of Bitcoin, and users of their app do not own Bitcoin directly. The users are buying shares of the community Bitcoin pile, and they can withdraw the

USD profits from any gain made. For many consumers, this is more than enough; however, if you'd rather own bricks of gold over a gold ETF, I would choose another option.

Exchanges such as Coinbase, Bitifinex, Kraken, etc. allow for their customers to buy Bitcoin directly from them as well as withdraw that BTC for their own personal use. I am also sure that very soon there will be many more avenues for purchasing BTC. Make sure to do your own research on any exchange, but at the moment this is the major distinction that exists.

Once you have bought your Bitcoin, it is very important that you know that **you do not *own* Bitcoin that is left on an exchange.**

You own this Bitcoin--on paper.

If you want to have full ownership of your Bitcoin, you must have your own Bitcoin wallet. You can then transfer your Bitcoin to your Bitcoin wallet and it will be safe.

Exchanges can get hacked, and once that happens, your Bitcoin is sitting there for the taking. If you are not using your Bitcoin for a trade, then I strongly advise you to secure your Bitcoin in an external wallet. If you don't believe me, ask people who have been in Bitcoin since 2014 about the Mt.Gox hack. The ripples (no pun

intended) from that situation are still being felt in the Bitcoin community.

Making Transactions

There's a slew of reasons why you could be making a bitcoin transaction and many of them require exchanging your bitcoin from one wallet to another--probably a merchant's--wallet. The process for this can be a bit scary, but once you get the hang of it, it's very easy.

Currently, there's some danger associated with transactions. I have a very good feeling that this will change as time goes on, but for now it **is critical that you are careful whenever you transfer bitcoin into and out of your wallet**. If you write the wrong characters or send your bitcoin to a non-bitcoin wallet, then the coins will be lost in the transaction (This applies to other cryptocurrencies as well). Some websites and wallets can stop you from sending bitcoin in the event that you entered an "invalid" address, but from the perspective of your wallet, they have no idea whether or not the address you sent is "wrong," these address are randomly generated, so it could be any variety of characters.

In the event of missent Bitcoin, you can rest assured knowing someone was very happy to receive their gift.

When transferring you need to figure out the address of the wallet you are transferring bitcoin to. Typically, there's either a CP Code (*above right)* or a text string. The string might look like this:

1PFYDqkSqRURPmVnS9Zry54sZdXGxvwoip. Both this string and the CP code link directly to my *actual* BTC wallet (so feel free to send me a few satoshis).

If you download a bitcoin wallet to your phone, you can scan the CP code, and directly send bitcoin to the address provided. This is probably the safest way to ensure that you do not make a mistake. But fear not, if there is no CP code, or you don't have that feature, you can likely copy and paste the wallet address text string. You should expect to see upper and lowercase letters as well as numbers; there should not be any special characters. If you are the person receiving Bitcoin, you should check your deposit address, and let the other person follow these steps.

You can share the CP code or the wallet address with anyone; however, **the private key should not be shared with anyone**. Seriously, absolutely anyone.

Your private key will likely be a series of random words. These words are what will allow for you to recover your wallet should it be lost (Remember, your wallet is virtual, so lost could mean, your computer had to be wiped, or your phone got factory reset, etc.). They are your only access to your wallet. If you lose these words and you're locked out of your wallet for whatever reason, then you will not be able to re-enter it and your coins will be lost.

You are your own bank.

Trading, Online Gambling, And Ref Links

The most popular method of accumulating more bitcoin would be trading. As I said before, there are plenty of Bitcoin exchanges, and when you make an account with these websites typically you have the ability to trade your Bitcoin as you would a stock market. Just like the standard stock market you have the ability to buy an index fund with Coinbase; you have the ability to trade Bitcoin against altcoins, like the forex market (Foreign Exchange); or you could trade Bitcoin futures. All of these are beyond the scope of this book, but you can certainly many resources about these topics online and in print media.

In addition to trading, you also have the option of playing online games for Bitcoin. There are gambling websites that use cryptocurrency for their funds. I personally know next to nothing about online gambling games, but I am also certain there is a lot of information out there.

Lastly, you will commonly see Twitter and Instagram accounts link you to different Bitcoin exchanges while encouraging you to register an account. The reason for this is, they get a kickback on the fees that the exchange charges you every time you make a trade. Typically the exchange fee will be less than 3% per trade, and the referral link will give the referrer something like 20% of the money that the exchange made on your trades. When the account has 100,000 followers, that becomes quite a hefty sum.

Contributing To The Community

Lastly, and arguably the most important way to get Bitcoin is to contribute to the community. Whether that means writing a book on cryptocurrency, building a project on the blockchain, a youtube channel, or simply integrating blockchain into your other ventures. If you create value, then, just like any other currency, you will position yourself to receive more Bitcoin.

This is the part that is entirely up to you, just note that there is so much that this technology can do, don’t limit your ideas. Think outside of the box. Use the blockchain in unique ways and help the space grow.

Chapter 8

What's Next?

It appears we've just about reached the end of our journey. By this point in the book, you should have a pretty comprehensive understanding of Bitcoin and the basics of the blockchain. A lot less complicated than you thought, right? What's next? What else is out there?

If you were to open a website like CoinMarketCap or some other site that compiled all of the information about different blockchain related tech, you would come to find that there is not just Bitcoin, but dozens of *coins*, and hundreds of *tokens*. What's the difference? Why do we need coins other than Bitcoin, what does the future hold for this technology, and how might this change the world we live in?

What's the Difference Between A Coin And A Token?

First thing's first, what differentiates coins from tokens?

A coin is a cryptocurrency that has its own dedicated blockchain. Bitcoin would be a coin, Ether (part of the Ethereum Network) is a coin, as well as many others. Many coins have the ability to have applications built on top of their dedicated blockchain. These applications are called *Dapps*, or decentralized applications. These dapps, often require the use of tokens in order to implement their functionality. Tokens are economic incentives present within a dapp to influence user behavior.

Simply, a coin has a dedicated blockchain and a token is found within a dapp. Coins have cross-contextual application and tokens have value within their decentralized network.

Tokenize Everything

Within the network, tokens can do so much. We have only begun to unlock the power of tokenomics.

Tokenomics is simply the study and design of token-based economies.

This sounds a bit far-fetched, why would you need to specifically examine the attributes of a token based

economy? Shouldn't the tokens simply function like money functions in our economy?

Well not quite. In our economy, the design of our currency gives it much more power as an item to spend than it does as an item to save. If you save dollar bills, due to the rate of inflation, they eventually become worthless. Saving money is important, but the value of that money progresses towards zero.

All this while living in a capitalist system. Anyone who's ever spent enough time in a coffee house knows of other economy models, typically socialism and communism. Is that all there is?

Cryptocurrencies aside, it's very possible that you've run into other economic models--token economic models even. In your classroom growing up, maybe there was some incentive system based around how many stars you received. You would perform specific tasks, these tasks would earn you a star. If the stars accumulated, you could get different rewards at different levels. This is likely the most basic, and most familiar tokenomic model you've experienced.

As adults, we participate with tokenomics models daily on social media. Most social media platforms function as follows: you create content, this content is viewed by other members of the platforms in exchange for "likes," the more likes you get, the more attention you get, and

this attention hacks into the dopamine receptors of your brain to reward you. Some platforms even allow for you to reshare posts, this being a higher reward than a simple “like.” Some platforms have upped the ante even further and integrated actual economy incentives into this attention-backed token economy

Believe it or not, our societal structure has quickly begun to shift because of tokenomic models. These dapps are using the blockchain and economic incentives--amongst other things--to influence behavior on their network. Whether that be Golem (GNT) who gives users tokens for contributing their computer’s computational power to its network. This decentralized network of computational power, creates a supercomputer, but for a far cheaper price tag.

When you’re designing a token economy, it’s very important to consider the behavior you want to transpire in your network. For example, if you have too few coins, each coin is worth significantly more, thus increasing the coins intrinsic value. The members of the network would be incentivized to not spend their tokens, but to hoard them instead.

Self Governance

Once you've begun to drink the blockchain kool-aid, you begin to see that there is unlimited potential found within decentralized applications. The transformative power that the internet promised, begins to feel like it will actually come to pass.

A global decentralized network, run by the people of this world, and for the people of this world. The potential to dissolve the nation state and create a world of self governance. But what will that look like?

Due to the decentralized nature of the blockchain, we have begun to work on models of governance that resemble our physical models of government, but are decentralized and tokenized on the blockchain.

Previously, we have taken a look at Poof-of-Work coins, but as time has gone on, more systems of self-governance have arisen. Mostly commonly, the proof-of-stake and delegated proof-of-stake models.

Let's begin with the PoW (proof-of-work) model. Energy expenditure is taken to be the digital equivalence of labor, thus providing value for the network. This value is also used as confirmation. Each of the nodes, check to see which chain is the longest, and that chain, because it has the longest amount of verified work, is considered to be the real chain. The simplicity of this method shines because there can be no dispute about which chain has done more work, and thus they reach *consensus.*

Proof-of-Stake has become another popular method for governance. Essentially, wallets can “stake” or put up their coins to the network. These coins cannot be used, but they represent how “invested” that party is in the success of the network. Thus, whenever a vote needs to be held, the wallets with the largest stake are given the most power in the decisions of the network. These wallets have the most to lose, so they should also be the most motivated to vote in favor of the network’s success.

From the PoS model, has come an alternative version, the Delegated Proof of Stake Model (DPoS). Just like the PoS model, nodes stake their coins, but now, specific nodes are chosen to be representatives. These representatives can be replaced if they lose their reputation in the network. These representatives have the majority of the voting power and they collectively make decisions for the network. This allows for consensus to be reached relatively quickly.

Real World Applications

When you see the rapid growth of cryptocurrencies, it becomes very easy to get tunnel-vision and to only conceptualize the blockchain as a means of verifying the transfer for wealth, but it is important to think outside of

the box and extrapolate on ways this technology can be transferred to other applications.

Let's start with the first principles:

1. Public ledger
2. Trustless verification
3. Decentralized

Any real world application that can benefit from these intrinsic properties of the technology are possible applications of the blockchain.

At the moment, The United States is having a gun control problem. There are many public shootings, and many people are dying. The American people do not want to give up their guns in totality, and why should they? The US is a very large country, it has all types of terrain, and all kinds of economic situations. Some people hunt for their food or their occupation. Attempts have been made to regulate guns to keep them out of the hands of those that are mentally ill or dangerous, but this becomes very difficult. Many stores can't keep track of these things, and some states have weaker gun regulation than others. This is where the blockchain could help.

If there were a blockchain that could verify the buyers ID, cross referenced with whether the buyer had any medical flags or criminal history. This whole process can be done very quickly and updated from any gun

merchant in any state--or country. This blockchain would create global accountability at the point-of-sale. Will this stop criminals who get their guns through other means? No, but this could very easily inhibit many of the criminals who simply walk into sporting goods stores and buy guns without even the slightest difficulty.

This wouldn't have to stop at the regulation of illicit materials (e.g. guns, medicine, etc.), you could use the blockchain to verify the supply chain or the legitimacy of precious gems. The blockchain could digitize the remnants of our physical papertrail. Ever have to search through all of your files for the *original* title to your car in order to sell it? Ever freak out because you couldn't find your birth certificate? Right now, we rely on notarized official documents, but why couldn't we just use a public ledger? If the dealership transferred the ownership of the car from the previous deed holder to the new deed holder on the blockchain, then that entire process would be unnecessary.

Closing Thoughts

There is no doubt that the blockchain technology will play a critical role in the future of our world. The ability to reliably verify trustless transactions is simply too great of a technological stepforward to not have a lasting impact. Similarly, cryptocurrencies aren't going

anywhere--though there’s no guarantee that any particular currency will survive.

Technological progress can be viewed as paradigm shifts brought on by transformative technologies. I can wholeheartedly say that we are experiencing the beginning of a new era. There is no doubt in my mind, that the blockchain will reorganize our world, and have a profound effect on the future world.

I am excited to see how this world unfolds, and I hope that this book acts as your first step into this new frontier.

Glossary

1:1 airdrop - marketing technique where a coin will distribute one of their new coin for each of the previously held coins their new coin forked from

51% Attack - an attacker owns over 50% of the nodes and can forge consensus.

Algorithm - system of rules that are followed in problem-solving or calculations.

Amaury Séchet - Creator of Bitcoin ABC

Bit - digital package of information

Bitcoin - the first widely adopted cryptocurrency

Bitcoin ABC - proposed Bitcoin fork

Bitcoin Cash - Bitcoin hard fork.

Bitcoin Unlimited - Proposed solution to block overcrowding

Block- area of the blockchain that permanently stores information about the network. Each block acts like a page in a ledger.

Blockchain - decentralized public ledger

Byzantine Fault Tolerance - When a distributed system can hide failure from different parts of the system. Prevents 51% attack

Caesar Cipher - a classic cryptographic cipher where you shift all letters over by a predetermined interval (e.g. A -> E, therefore all are moved 5)

Cash system - *a monetary system that can be used as a unit of account, medium of exchange, and store of value.*

Cipher - *a code to disguise information*

Ciphertext - the jumbled text left after a cipher was applied

Coin - *a cryptocurrency with a dedicated blockchain (e.g. bitcoin, ether, monero, etc.)*

CoinMarketCap - *website that* compiles coin and token data

Cryptocurrency - *digital form of currency that is secured via cryptography.*

Cryptography - the art of writing or solving codes

Cryptosphere - the cryptocurrency online space

Currency - a cash system that contains the following six properties: durability, portability,
Divisibility, uniformity, limited supply, and acceptability

Dapp - decentralized application built on blockchain

DDoS attack - denial of service attack.

Decentralized **-** transferring authority away from central management, providing more autonomy.

Deflation *- the decline of prices for goods or services when the inflation rate falls below 0%. Occurs when the supply is fixed.*

Delegated proof-of-stake *- A proof of stake consensus algorithm that uses delegates—chosen by the community—to vote on behalf of the broader network. This increases the speed of consensus, but provides more centralization.*

Double-spending - Using the same cryptocurrency for two transactions

Encode *- to apply a cipher*

Ether - coin on the Ethereum blockchain

Fiat *- currency that is backed by the government that represents it, as opposed to being backed by a commodity (such as gems or precious metals)*

Fractional reserve banking - Banks keep a fraction of the money they store in reserve, and lend the rest of it to customers. Increases total monetary supply, but adds no real value per additional dollar.

Hard fork *- an abrupt change to a codebase, that causes two different versions of the original code to exist. This change is not compatible with previous versions of the software.*

Hash *- a computer function that maps information of any size to a unique and seemingly random string. For a hash to be useful, it must be able to be decoded given the appropriate information.*

Hyperbitcoinization - When use of the bitcoin protocol is suddenly adopted due to the i

Hyperinflation - when inflation reaches the point that money becomes almost worthless.

Inflation *- The increase in the price of goods and services over time.*

Jan Lanksy - created six rules that define what makes a cryptocurrency

Jihan Wu - creator of Bitcoin Cash (BCH)

Joseph Poon *- co-creator of the Lightning Network.*

Kazaa - P2P network from 2006

Ledger *- digital record of information*

Lightning Network - Adopted solution to Bitcoin scalability

Limewire *- P2P network from 2010*

master - *the permanent branch of code that represents the production-ready state.*

Medium of Exchange *- property of a monetary system that allows value to be transferred from one party to the next.*

Mining *- using computing power to verify information on the blockchain*

Moore's Law - the observation that the number of transistors in a dense integrated circuit doubles about every two years

Mt.Gox *- Cryptocurrency exchange that was hacked in 2015.*

Napster *- the first P2P network. Founded in 1999*

Peer-to-peer (P2P) *- a network architecture that does not store the information solely in a centralized server. The information is distributed amongst all of the network's constituents.*

Plaintext - a decoded message

Private key *- your password*

Proof-of-stake *- governance algorithm that reaches consensus by putting up your coins to demonstrate your "stake" in the network. Users with more coins at-stake, have a larger vote.*

Proof-of-work *- consensus algorithm that uses digital labor to verify transactions on the blockchain*

Push *- to submit a change to a codebase*

Ref link *- a referral link to a cryptocurrency exchange. Gives the link sharer a percentage of the referee's network fees*

Repository *- a place where code is stored*

Robinhood *- brokerless stock trading app. Founded in 2013*

Roger Ver *- "Bitcoin Jesus" and avid support of Bitcoin Cash*

satoshi *- smallest denomination of a Bitcoin. There are 100,000,000 satoshis in one Bitcoin.*

Satoshi Nakamoto *- pseudonym held by the creator(s) of Bitcoin*

Sean Parker *- Founder of Napster*

SegWit *- "Segregated Witness," adopted solution to transaction malleability (see: transaction malleability)*

SegWit2x *- The compromise soft fork Bitcoin adopted in order to accommodate those that thought block size should be increased. This fork doubles the 1MB block limit.*

Server *- centralized store of computer data.*

Smart contracts *- a computer protocol designed to enforce a contract.*

Soft fork *- backwards compatible change to the blockchain.*

Store of value *- For something to be a store of value, it needs to be able to preserve wealth. A currency that cannot preserve value, quickly becomes worthless.*

Technological Adoption Curve *- This is the rate the the general public takes to begin using a new technology. There are 4 distinct phases: Innovator, early adopters, early majority, and late adopters.*

Thadeus Dryja *- co-creator of LIghtning Network*

Token *- a cryptocurrency that does not have its own blockchain. Typically, they serve to raise funds or to incentivize behavior on a network.*

Tokenomics *- the study and creation of token based economies.*

Transaction malleability *- a technological flaw that allows for transaction information to be changed by hackers.*

Unit of Account *- the ability for wealth/value to be measured. You should be able to gauge the value of goods or services. If a currency cannot do so, it will be difficult to understand price and profit.*

Wallet *- digital container for cryptocurrencies.*

Wallet address *- the public "location" of your digital wallet*

Watchtower node *- a trustless third-party node within the Bitcoin Network tasked to confirm the validity of transactions within a two-way payment channel.*

Whitepaper - *a technical* introductory paper that introduces a technology.

References

https://cointelegraph.com/Bitcoin-cash-for-beginners/what-is-Bitcoin-cash#story-of-the-hard-fork

https://satoshi.nakamotoinstitute.org/quotes/economics/

https://Bitcointalk.org/index.php?topic=130619.0

https://www.investopedia.com/terms/c/currency.asp

https://lightning.network/lightning-network-paper.pdf

https://golem.network/

https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

https://blockgeeks.com/guides/dapps/

https://bitcoin.org/en/faq#who-controls-the-bitcoin-network

https://bitcoin.org/en/faq