

BITCOIN | EVANGELISM



PLANTING SEEDS FOR THE
DECENTRALIZED REVOLUTION

Brian E. De Mint

Bitcoin Evangelism

Copyright © 2022 by (Brian De Mint)

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without written permission from the author.

Hardcover: ISBN 979-8-9863463-1-1

Softcover: ISBN 979-8-9863463-0-4

eBook: ISBN 979-8-9863463-2-8

International Black & White: ISBN 979-8-8406191-1-7

Printed in USA by 48HrBooks (www.48HrBooks.com)

Edited by Cindy Draughon

Check out my books at www.FreshlyMintedBooks.com

Connect with me via social media. I love answering any follow up questions that you may have.

Twitter: @BrianTheMint

Instagram: @Brian.DeMint

Facebook: @Brian.DeMint.One

Email: brian@freshlymintedbooks.com

Website: www.FreshlyMintedBooks.com

Dedication

To the Lord. I am grateful for the grace He has given me and that he lets me live a life full of passions that I get to pursue.

To Mom. Thank you for being my guiding light.

To Alyssa. Without you, this book would not have been written.

To the Church. May this be a resource for believers. A financial strength to match their spiritual strength will make them more resistant to outside pressures from this world. If those pressures ever become strong enough, BTC will be a valuable tool to continue God's mission in a volatile world.

Table of Contents

Foreword	7
Introduction	11
One: Resistance to Adoption	21
Two: Getting Familiar with The Terms	45
Three: The 8 Qualities of Sound Money-and the New, Secret 9th Quality	85
Four: The Nine (ok, Ten) Tenets of Bitcoin	111
Five: What Makes Bitcoin So Special?	131
Six: Breakdown of Crypto Asset Classes	175
Seven: Problems With the Current Financial System	187
Eight: A Brief History of Currencies & The Inflation Formula	221
Nine: Digital Asset Investment Principles	237
Ten: Why Does Bitcoin Have Value?	282

Table of Contents

Eleven: <i>What are the Limitations of Bitcoin?</i>	320
Twelve: <i>The Capitalists and the Communists Will Both Be Satisfied</i>	328
Thirteen: <i>Short Answers to Common Questions</i>	340
Fourteen: <i>Short Answers to Not-So-Common Questions</i>	366
Fifteen: <i>Reliable Sources in Bitcoin</i>	374
Conclusion	378
Bitcoin Whitepaper	381
Find The Bitcoin Wallet In This Book	390
Citations	391

Find The BTC Wallet In This Book

On May 31st, 2022, I will add \$1,000 USD worth of BTC to the wallet at the market price on that day.

The public address is

**bc1q60dlvz2khfp9j72as2ksz8w8mp9x9k0jh2lk73
bc1q35dwtv2yswnurj9jv6eq4rz4nyxa2ft5rnm7rx**

Please go to www.Blockchain.com to verify for yourself that the funds are in this wallet.

Throughout this book you will read about the new innovations being ushered in by Bitcoin and blockchain. These new technologies will allow for novel and interesting concepts. One such concept is this: I have hidden a BTC wallet within this book. This is the first book in history to do this. You are participating in something that no group has ever done before.

There are a few reasons why I am doing this. First, it's to encourage individuals to really dig into the text. You won't just find this wallet by casually breezing through the pages. Hopefully, this will cause readers to fully digest the material and learn it more concretely.

Secondly, I want to display a rudimentary lesson in how BTC wallets work and some of the creative ways they can be stored and secured.

Third, I want to prompt people to think outside of the box when it comes to this new frontier in technology. We are blessed to be at a moment in history where new trails will be blazed. Those that can understand this new technology, and find new and innovative ways to apply it, will benefit the most from it.

Instructions for how to join in this real life treasure hunt are in the back of the book. Godspeed!

Foreword:

“Hey man, you want to jump in and train with us?” were the first words Brian De Mint said to me. I was a two-stripe blue belt who hadn’t trained in jiu jitsu for over five years and I had my doubts about getting back into the sport as an older, out of shape guy. I woke up early that morning to watch the 7:00 AM jiu jitsu class and, after seeing a few rounds of high-level grappling, I was ready to dismiss the thoughts of getting back into the sport, and just leave. But Brian’s welcoming gesture and the friendly conversation that followed changed my mind. I decided to stay and give it a shot. Little did I know how that day would impact my life and my family’s financial future.

Jiu jitsu is now a lifestyle for me, as it is for Brian. We study jiu jitsu countless hours a week, test our skills competing at tournaments, our kids train, and conversations with our wives probably include the words “rear naked choke” more than they should. Brian and I were even promoted to the rank of brown belt on the same day. Needless to say, we spend a lot of time together and have learned a great deal about each other’s lives and interests. When I first joined the jiu jitsu school, I heard Brian and our former instructor talk about bitcoin. I didn’t understand bitcoin at all and considered it magic internet money used only to buy drugs on the Silk Road website. My opinion changed as I listened to these guys that I respected discuss *different* aspects of bitcoin. It soon became obvious to me that my perception was incorrect, so I dipped my toes in the water and bought some bitcoin. This was mid-2017. Before I knew it, my initial investment had doubled.

As the price of bitcoin increased, so did my questions. Thankfully, Brian had a deep understanding of bitcoin and was patient enough to answer my questions, some of them twice, without making me

feel like I was wasting his time. As I learned more details, I bought more. Then, seemingly out of nowhere, the bear market hit in December 2017 and bitcoin's price plummeted. As it continued to crash, I thought it might be the end of bitcoin and I stopped buying. As I contemplated my exit strategy, Brian continued to hold his bitcoin and acquire even more at the depressed prices. Did he know something that I didn't?

Throughout the 2018 bear market, Brian held firm to his beliefs. This prompted me to dive even further down the bitcoin rabbit hole to see what I had missed. As 2019 approached, and after countless conversations with Brian, it finally clicked. I saw that Bitcoin was much more than just a way to make some quick money. It was created to fix the broken fiat money systems where governments can print unlimited amounts of their currency to sustain their excessive spending, and as a result, inflate away the value of our money. After coming to this realization, I began converting more of our dollars into bitcoin.

Were there times when doubts crept in? Sure. Back then, untruths spread online about bitcoin caused me to second guess my thesis but Brian, through his thoughtful teaching style, took the time to explain the facts. There is so much more to bitcoin than meets the eye so it takes time to truly absorb it all and appreciate that bitcoin is unlike any other cryptocurrency. Brian lives and breathes this stuff, spending an inordinate amount of time keeping apprised of cryptocurrency developments. It took me a while, but these days I absolutely understand Brian's conviction. When the price of bitcoin drops, I see it as a great opportunity to buy more at a discount. When a family member, friend, or acquaintance brings up bitcoin, I jump at the opportunity to join in the discussion. Throughout this journey, I shared my newfound knowledge with my wife and got her into bitcoin too. Together, we agreed bitcoin is a world changing technology that cannot be confiscated or debased and that we would not sell any of this scarce asset unless it would change our lives. Well, that moment arrived much sooner than we expected.

In August 2021, we used a portion of our bitcoin profits to pay off our home mortgage. We live in Southern California where homes like ours cost \$900K+ so this was truly a life changing moment for us. We purchased the property in 2016 and paying it off so quickly was an

absolute blessing. I've heard the arguments against paying off your mortgage early (like getting a better return through investing the money) but let me tell you, the peace of mind knowing that no matter what happens in the future my family's housing is taken care of cannot be understated. Bitcoin brings freedom and paying off our home mortgage was a taste of that freedom.

We are now debt free and we can refrain from selling our remaining bitcoin. As a matter of fact, we continue to buy more bitcoin as we firmly believe that it will replace gold as the default store of value and that it will likely become the global reserve currency one day. We believe in it so much that we have taken extra precautions to secure and protect our bitcoin. We also moved a portion of our bitcoin to sites that provide annual yields of ~5%, producing a nice passive income stream, like an investment property but without the headaches. Bitcoin is an opportunity to create generational wealth for our family. A pristine asset that can be passed down from generation to generation. It can do the same for you, too, but it takes more than just blindly buying bitcoin; You must educate yourself. Bitcoin's price is highly volatile and if you lack a firm understanding, then fear can cause you to lose confidence and sell during the temporary downturns that inevitably come. Please, don't be that guy or girl.

While having lunch with Brian at a friend's restaurant, a gentleman walked up to our table and said to Brian, "We met before and I'm really sorry I can't remember your name. We had a great conversation about bitcoin and, if you're available sometime, I would love to talk to you more about it." That kind of random stuff happens to Brian because he goes out of his way to help others understand bitcoin, even relative strangers. I wasn't surprised that the gentleman remembered their impactful conversation and was compelled to approach, even though he couldn't remember Brian's name. I have felt the same compulsion over the years, wanting to download as much of Brian's bitcoin expertise into my brain as possible. That is why I am so glad he took the time to put his thoughts down on paper. *Bitcoin Evangelism* is an excellent resource for that gentleman, for me, and for you.

We are still early in bitcoin's adoption, but progress is advancing rapidly with major financial institutions now getting involved and one country already adopting it as legal tender. Heck, there are even professional athletes getting paid their salaries in bitcoin. Developing a solid foundation will prepare you for this nascent technology that has begun to disrupt the legacy financial system. Whether you're new to bitcoin and want to understand why it deserves your attention, or you're already into it and want to broaden your knowledge, Brian's wisdom on the topic is a great place to start. *Bitcoin Evangelism* is the culmination of Brian's years of experience diligently studying cryptocurrencies and generously educating others. As a passionate OG in the bitcoin community, his knowledge is incredibly extensive, and his conviction is extremely contagious. I hope this book is a blessing to you and your family, as learning from Brian has been for me and my family.

Erik Goodin

Multiple time IBJJF Jiu Jitsu
World Champion

Introduction

“Wealth is your time, and money is just a representation of your time. Wealth is never destroyed, it is merely transferred. On the other side of every crisis (and technology revolution) there is an opportunity.”

- Mike Maloney,
Economist

If reading Milton Friedman is like wearing a fine suit, then this book would be like the millennial wearing joggers and a hoodie to the office, which is very much the culture of Bitcoin. Bitcoin is only more recently being adopted by those in suits and ties. It was fostered by a group of people that would be very uncomfortable in an executive board room. But that's one of the wonderful things about Bitcoin, it's not just for computer nerds or wall street types, it's for everyone; everyone has equal access. Equal access to a monetary system is a novel concept in and of itself. No monetary system in history has been open to everyone, until Bitcoin.

The terms Bitcoin and blockchain may be used somewhat interchangeably, but that is an oversimplification. Bitcoin is both a crypto asset/currency and a network/protocol. Perhaps Satoshi Nakamoto (the creator of Bitcoin) should have branded these as two separate items (such as BitNetwork and BTC) but what's done is done and we must bear with having to consistently clarify whether we are referring to the asset or the network. Please keep an open mind as you read on and go with the flow as we drift back and forth while discussing the merits of both the novel asset and the revolutionary network. Some things may sound redundant,

but that is by design to create a deeper and more well-rounded understanding of these ideas. We will revisit some ideas because most require a layered and more nuanced understanding.

Grasping these concepts is important for anyone looking to navigate the next chapter in human history. People who lack understanding or have bad information will inherently make poor decisions. Not because they are bad or stupid, but because they simply do not know. This is particularly true when it comes to financial and economic matters. Maybe because it's boring or maybe because it's perceived as confusing.

Someone stranded on a life raft in the middle of the ocean might unknowingly drink saltwater to quench their thirst. To the person dying of dehydration, saltwater looks exactly like what they need. They continue to drink it thinking it is solving the problem, when in actuality, the more they drink, the more dire their situation becomes. The person on the raft must first learn that saltwater is toxic and then they will be better equipped to make decisions about how to survive and ultimately thrive.

In the same way, people continue to think our current financial system is somehow the fix to their problems - more government spending and more safety nets. Big banks and crony capitalism. Most people do not understand the toxicity because this system is all that most of us have ever known. It's similar to the saltwater that looks like the solution but is ultimately what poisons us.

I have a deep passion for helping people to help themselves. I have faith that when people are equipped with good information, they can make better decisions for themselves and their family. Selfishly, when others in my society flourish, more opportunity is created for me and my family as well. This way of thinking prompts me to call myself a Bleeding Heart Capitalist. This is a very big idea that perhaps requires its own book.

This book is not intended to sound alarmist. And because I talk so positively about how Bitcoin and blockchain are potential solutions

for some of these problems, it may come off as though I am rooting for the current system to fail. I am not. Balaji Srinivasan said it perfectly when he stated,

“The guy with the parachute doesn’t want the plane to crash but he’s prepared in case it does.”

My purpose in writing this book is to let people know that blockchain technology will be an essential part of the future of all societies, and those who understand it early will benefit most greatly. I first learned about Bitcoin in 2013 and have literally spent some portion of every day since then either studying the technology more deeply, working in an executive role in a blockchain project, reading new project whitepapers, or studying innovations and news within the industry. None of the information in this book is intended to be investment advice. But rather, it is meant to pass along the product of these thousands of hours of study and provide an educational groundwork for understanding a shifting paradigm. Though that level of commitment may not be palatable for many, reading this book might be. And that’s what *Bitcoin Evangelism* is, it’s an aggregation of thousands of hours of research and experience in the digital asset world.

I have been in the industry through several boom-and-bust cycles and noticed each time Bitcoin and crypto prices are in an upward trend, I receive more calls, texts, emails, and direct messages from friends, peers, and even old acquaintances from high school, who are reaching out for answers to their questions. They are just beginning to dive into Bitcoin and are feeling overwhelmed.

Other friends who are “seasoned veterans” (in a new industry a veteran may be someone with as little as three years of experience) in the crypto industry have similar stories of friends reaching out in large numbers. We all do our best to help people understand Bitcoin and blockchain more fully but often the curious individual new to the industry may not know what questions to ask to get the information they want. I believe that understanding things before you try them is a generally good position to take. But beware of “paralysis by analysis” - a

phenomenon that happens where someone fails to adopt a new technology because they believe they need to understand absolutely everything about it before using it.

While this is true if you are looking at bitcoin as an investment, it isn't necessary if you are looking to use Bitcoin as a technology. For example, you probably send emails, correct? But do you understand how SMTP (email software protocol) works? If you're like most people, you don't. All you know is that when you type something and press send, that email will be received by whomever you wish. Sometimes just jumping in and using a technology with small stakes is the best way to go. I am a praying man and in church we have a saying, "Sick people shouldn't wait to get well in order to go to the hospital, neither should a sinner wait to stop sinning in order to go to church." The takeaway here is that we can always find reasons to not better ourselves or adopt a new way of doing things, but the sheer fact that you are reading this book indicates that you are taking that difficult first step. The next challenge is to read all the way to the end.

For those who do wish to understand Bitcoin and blockchain more broadly, this book can be a resource for you. Once you become one of those "seasoned veterans" I referred to, you can give this book to someone who comes to *you* with a laundry list of questions. Blockchain is a deep and wide subject, but once you familiarize yourself with the concepts throughout *Bitcoin Evangelism*, you will understand more about Bitcoin and how our monetary system and macroeconomics work than 99.99% of the world - that's not an exaggeration.

A little bit about me. I grew up on Sovereign Way in Riverside, Ca. From a young age I was acutely aware of the concept of individual sovereignty because I repeatedly (as children do) asked my parents questions like what our street name meant. My mother always took a little extra time to explain these kinds of things to me. Her willingness to simply explain complex issues has shaped my worldview even to this day. In this particular case, understanding the value of individual sovereignty was a concept that has been constant throughout my life.

I come from a family of money-makers. At least my last name - De Mint - indicates so. I grew up in a middle-class family with a father that died of a drug overdose and a mother that wouldn't accept the bad

circumstances in my life as an excuse for me and my brother to fail or be lazy. So, I don't particularly come from wealth, but I also didn't grow up on the streets by any means. Regardless of our recent family history, my family name indicates that at some point in our lineage we may have been European nobility. "Mint" indicates that our trade was coin minting, or banking, and "De" is a term reserved for nobility that means "from the house of". So my family name literally translated means *From the House of Money Making*.

This was pointed out to me by my middle school history teacher, Mr. Noller. After digging further, we discovered it was accurate. Ever since the day Mr. Noller pointed that out to me, I had it in the back of my mind that my calling had something to do with entrepreneurship or finance - but I despised the banks and much of wall street, even from a relatively young age. So, I went with entrepreneurship. That journey eventually led me to Bitcoin and blockchain. When I finally learned about Bitcoin in 2013, as a boy with a name that meant "coin minter" who grew up on Sovereign Way, a light bulb went off and I thought to myself, "This is it! Self-sovereign money. This will change the world and people need to know about it." I believe everyone has a shared purpose and that is to glorify God, and one of the ways we do that is through our passions and our work. For me, helping people understand macro finance and, more specifically Bitcoin, seems to fit my destiny, calling, or whatever you want to call it.

For three years I was privileged to be able to work as the Chief Marketing Officer for Atheneum Blockchain, an education-centric blockchain startup. As a huge fan of the Bitcoin Whitepaper, it was an honor to be able to co-write the Atheneum whitepaper and develop the roadmap for that project. While I fully believe in the noble mission of Atheneum and its goal to provide a decentralized free market for educational and learning content to everyone, I resigned in late 2021 to write this book.

During the 2012 presidential campaign, incumbent Barack Obama notoriously said, "If you've got a business, you didn't build that." He preceded that comment by stating that the work of other people (like those that built your bridges and roads) enabled entrepreneurs to start

their business. It came off as tone deaf to a generation of small business owners that had just weathered The Great Recession. It was used as political fuel against him to label the president as someone that was anti-business and disrespected the sacrifice of small business owners. It was seen as one of his biggest verbal blunders of the campaign. As an entrepreneur, I was offended because I took great pride in the fact that I had built a business, had thousands of happy customers, and provided jobs for people in my community. As a Libertarian and someone who did not vote for President Obama, I was eager to lambaste him over this comment.

As time went on, I was able to remove myself from the political hostility of that campaign season and see some truth in his comment. While I don't believe we should undermine the contributions of business owners, I do think it's important that we take stock of what people and influences have shaped our lives. We must also realize that we are privileged to live in a time where we benefit from the innovation and labor of all the generations that came before. Sir Isaac Newton said we see further (and can be so successful) because we "stand on the shoulders of giants".

We are at a crossroad in history where we can better the lives of our communities, our culture, and our world if we seize this critical moment where innovation has given power back to the people in the form of blockchain technology. Going down new roads can be uncomfortably scary and, truth be told, most people will avoid that road altogether. Acknowledging the parents, family, teachers, pastors, books, podcasts, thinkers, and other sources of influence in our lives grants us humility. A humble mind and open eyes allow us to learn new things. This book's aim is to make understanding blockchain straightforward and simple in hopes that we can remove the discomfort and anxiety that comes with crossing into uncharted territory.

Society is seeing the biggest political and values polarization in recent history. Part of my motivation to write this book also comes from the belief that the polarization of our country, our communities, and our houses of worship, is being driven by monetary forces. I mean, is it that big of a stretch to think that money affects every aspect of our lives?

"The future is not about left versus right but rather up versus down. It's about those with power versus those without it. It's about centralization versus decentralization."

- Maajid Nawaz,
Former Muslim Extremist.
Chairman of Quilliam,
a counter-extremism think tank

Over the coming two to ten years we will see the biggest wealth transfer in human history. At its core will be blockchain. Furthermore, this period will usher in a technologic layer that the Founding Fathers of America never had at their disposal to ensure that their ideals of liberty were preserved. While the Constitution is a wonderful document, humans always have the ability to act out of accordance with it. It is attributed to Mayer Amschel Rothschild (of the Rothschild banking dynasty) that he once said,

"Permit me to issue and control the money of a nation, and I care not who makes its laws."

Human systems are always vulnerable to human error and corruption. Algorithmic systems based on mathematics and rules that can be viewed by anyone at any time, provide a novel solution to the age-old problem of bias, wickedness, and corruption.

Blockchain ensures that rules and fair systems are always maintained with mathematical precision. Blockchain isn't only capable of democratizing finance, it can democratize education, social media, the news, voting (verifiably) and more. The hegemonic elites have traditionally had an upper hand in these historic transitions and usually rig the game in their favor, but blockchain technology provides a unique opportunity, through its decentralized nature, for regular people like you and I to front run this transition and benefit from it far greater than the establishment and those that uphold the status quo. My prayer is that this book is used as a resource for the average individual to be equipped to

ride this wave and benefit their families and their communities for generations to come. *Bitcoin Evangelism* is a tool for you to learn from and then pass along to share information about this new paradigm that has the ability to transform the world for the betterment of humanity.

And lastly, if we want a better future, it is imperative to understand our world's current economic systems. These financial systems are broken and therefore create pain, inequality, and suffering. While we may live in a Republic, our financial systems operate outside the ideals of individual liberty, equality, and democracy. While left, right, and center have much to disagree on in our current culture, I believe finance is one of the few remaining areas where our American ideals overlap. This means we can work together in unity to build a new system to migrate peacefully to rather than tearing down the existing one. R. Buckminster Fuller said it best when he stated,

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.”

By becoming a Bitcoin Evangelist, you get to play a role in ushering in the new model and take part in a historical movement, the likes of which the world has never seen before.

“Bitcoin is going to change the
world because the world can’t
change Bitcoin.”

- Jack Mallers,
CEO of Strike

Chapter One:

Resistance to Adoption

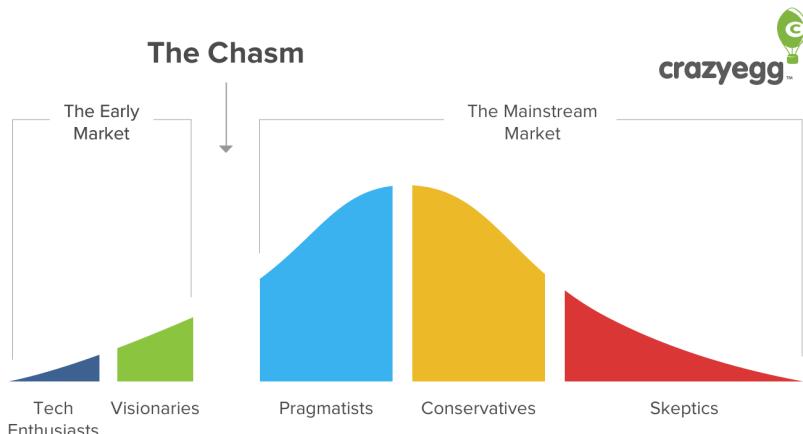
“If you know nothing else about the future, you can rest assured that dramatic changes will be neither welcomed nor advertised by conventional thinkers.”

- The Sovereign Individual,
1997

When we look back at the history of new technologies, we find there is almost always prodigious resistance. This resistance can come from existing enterprises that do not want to lose market share to the new tech. It can come from those who fear the mysterious nature of new things or that simply do not like change. Resistance may come from a place of ignorance or individuals being unable to see past current limitations of the technology to what its potential is. Or the resistance may come from seeing a need for further innovations within the tech that do not yet exist. With Bitcoin it is no different. In fact, there may be even more parties interested in suppressing and stifling innovation in the blockchain space because the transfer of money and value along with the novelty of digital scarcity affects every single industry. It affects politics. It affects academics, ethics, banking, science, and so much more. And because it is a new technology that people also see as an investment, they may be nervous of potential financial loss.

Typically, we see two types of people/entities that resist novel tech adoption: those that ultimately acquiesce and jump on the bandwagon, and those that will be made obsolete or irrelevant. The chart below by CrazyEgg does a great job of illustrating what the adoption cycle of a new technology looks like. As we will see in the following

sections where we look at various technologies, the tech enthusiasts and visionaries always face a lot of skepticism. They are seen as the heretics to current consensus. They are viewed as smart people that are a bit crazy, and their ideas are a little too big and grandiose. Initially, the incumbents will attempt to diminish the new challengers by warning that they should not be taken seriously.



When the challengers start to make headway, the current establishment ridicules them and resorts to arguments based upon their own authority (ie: “Experts say that kerosene is more efficient than electricity! Are you going to disagree with the expert and believe some new electricity-pushing loon?”). As the challengers make even more progress, they will be accused of dealing in misinformation or be labeled as conspiracy theorists for even attempting to challenge the status quo. The establishment may even invoke scare tactics to worry the public about the new technology or go so low as to call the new field one of criminals and outlaws.

History shows that these tactics were unsuccessfully used many times in the past, and yet they are still used against Bitcoin today. I’m assuming that the establishment hasn’t done enough reading of history. I also don’t think they’ve done enough study of Bitcoin. In a US House

Financial Services Committee hearing, Chairwoman Maxine Waters referred to Bitcoin as “BitCom” throughout the hearing as she spoke antagonistically of the new tech. Maybe she assumed BitCom was a website? Regardless, the establishment that is attempting to suppress innovation is already becoming less relevant as subsequent congressional and senatorial hearings have become very praiseworthy and forward thinking on blockchain, which is in stark contrast to hearings from 2020 where ignorance and objection were the going sentiment.

New technologies will always meet resistance for a variety of reasons from those that simply like the way things are to those that stand to benefit from the status quo, and from those afraid of change to those that lack foresight. While we are starting to turn the corner from flat out rejection of Bitcoin to a more balanced conversation, there is still some way to go. Let’s take a look at some of the innovations that define our current world but were once viewed as new, mysterious, and scary. My challenge to you is to see if you can find any similarities between the history of these technologies and that of Bitcoin and blockchain.

“It is difficult to get a man to understand something when his salary depends on his not understanding it.”

-Upton Sinclair,
Author and Muckraker, 1934

Electricity

The history of electricity is a fascinating one. Early light bulbs were too powerful for homes and thus there was little adoption. Thomas Edison’s incandescent light bulb was a game-changer that made it possible for homes to benefit from the power of electricity. It took decades for appropriate safety measures to be developed though. Early electrical wires were bare, unsheathed, and ran along walls and floors. This led to frequent electric shocks and fires. Would you have electricity in your house if there were exposed wires everywhere for your two-year-old child to touch?

In the early days of electrical power there were no standardized outlets. The only regular type of outlet was for a light bulb. Even once

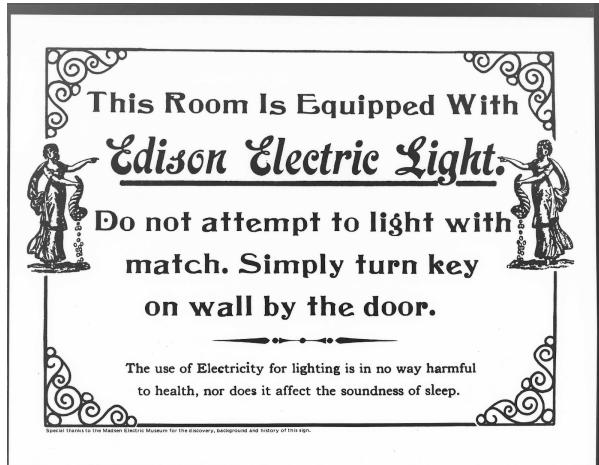
outlets were developed, they weren't grounded and were metal on metal. This meant that any time you plugged something in or unplugged it later, sparks flew.

Early adaptations of the technology missed the mark entirely. Various forms of shock therapy were used to treat a wide variety of diseases - albeit unsuccessfully. One such patent shows a rather misplaced optimism in the potential of this new technology. The Electrical Spray and Vapor Bath's inventor describes his invention here:

"The principal object of my invention is to provide a simple bath in which electric currents may be applied to the human system in the most efficient manner and in the greatest possible variety of ways..."

Yes, you read that right. An electrified bathtub. And this was in an era with no sheathing on wires, no electrical breakers or surge protectors. A bathtub with electrical currents sounds more like one of Jigsaw's contraptions rather than a therapeutic remedy. We see similar projects like this in the crypto space. Developers don't even fully understand what the future implementations of the tech will be, so they just build. Some projects have no actual utility, while others are scams or are poorly built making them vulnerable and dangerous to investors. And yet other projects are innovative and world building. Skeptics and electricity naysayers were eager to highlight inventions like The Electrical Spray and Vapor Bath because it supported their myopic narrative, while they ignored viable innovations like the incandescent light bulb.

While the electrified bathtub was an obviously bad idea, other uses of the technology that would later go on to gain popularity had growing pains of their own. The telephone, powered by electricity, transformed communication even though many early reports of its danger made the rounds. Picture reading the daily newspaper and seeing a headline such as: "Man Picks Up Telephone, Dies From Shock." The uphill public relations battle faced by early proponents of electricity must have felt like a losing battle. If fear wasn't enough to be an impediment, then certainly ignorance was. Check out this sign from Edison General, instructing users to make sure to flip the light switch rather than trying to light their indoor light bulbs with a match.



Before electricity, the juggernaut of the indoor lighting industry was John D. Rockefeller's kerosene lamp. His company, Standard Oil, was the world's biggest company and made their fortune by providing kerosene to every home in America. So, when Thomas Edison's incandescent light bulb began to replace kerosene lamps, Rockefeller took notice. Almost as quickly as kerosene had extinguished the previous incumbent, camphene, two decades before, electric lighting dimmed kerosene's market share as households switched on electric lights.

Standard Oil did everything they could to fuel anti-electricity propaganda. Oddly enough, twenty years before, kerosene had to fight off its own bit of unfavorable press. As kerosene became more popular, stories of house fires from kerosene-fueled lamps stoked fear among the general population. Standard Oil learned that fear was an effective way to suppress this new and promising industry.



Ultimately, electricity was such an efficient alternative that it won the day. Standard Oil relented, not only because it was losing the battle to electricity's growing adoption, but the petroleum industry found a new innovation that would drive an even greater demand for its resources - the automobile.



Bicycles and the Horse & Buggy vs the Automobile

The advent of the first functional automobile by Karl Benz in 1886 was not an immediate threat to the popular forms of transit at that time. The horse has been used for transportation since 2,000 BC so to say that it had a bit of a headstart on the automobile is a bit of an understatement. While various forms of horse powered travel had existed for almost that same amount of time, the formal Horse & Buggy industry had existed since the late 1600s. Karl von Drais developed the first bicycle in 1817. In the renowned book *Extraordinary Popular Delusions and The Madness of Crowds*, author Charles Mackay details the great British bicycle bubble during the late 19th century. Like the .com bubble of the early 2000s, bicycle companies were being valued at many multiples of their revenues, let alone profits. Even after the bubble burst, the bicycle industry had become a well-financed industry around the world and these companies were the tech powerhouses of their day.

It's easy to see why both the Horse & Buggy industry and bicycle manufacturers would be nervous as automobiles evolved from a vanity and a novelty to become more reliable, gaining greater market share. While the automobile would not even be close to achieving its greatest efficiency by 1900, these incumbent industries could plainly see that their technologies would eventually be beat out by further maturing in the automobile industry. This led them to use their established power to do whatever they could to tamp down this emerging sector of the market. They used both the power of political lobbying and the more cunning tactic of anti-automobile propaganda.

One such famous law passed with a tilt toward stifling the adoption of the automobile was early speed limits. The earliest legislated speed limits for cars were 12mph in the city and a blistering 15mph in the countryside⁽¹¹⁾. Since speed was one of the clear advantages of even the early automobiles, it made sense to suppress this edge over traditional modes of transportation. Even with these terribly slow speed limits, drivers were also required by law to slow down further and evade horse drawn carriages to not scare the horses. Per the law, it was clear that the Horse & Buggy was the privileged vehicle on the road.

Perhaps the silliest legislation that was hijacked and used to stifle the automobile was the “red flag law”. This was a law for trains as they

passed through cities. At the time, this law made sense for locomotives because there were no crossing rails like we have today. In those days, trains often traveled right through the heart of a busy city. So, legislation was developed that a “flag boy” needed to walk in front of the train and warn people to get out of the way.

Although cars were much more akin to the horse drawn carriage than a train, as is seen in the common name for cars, the *horseless carriage*, legislators moved to have this law apply to automobiles. This was a sneaky way to cut down the already horrendously slow 12 mph speed limit to the walking pace of about 5-6 mph. Plus, the added cost of paying a personal flag boy made driving just that much more out of reach for most people and even those that had the means, would be sure to face frequent frustration while using their new technology.

Early automobiles most certainly lacked any of the safety components that modern cars enjoy. So, to say they were totally safe would be disingenuous. But rather than seeing the potential to innovate in this area, the shortcomings were widely publicized and used as anti-automobile propaganda. The ad below reads “Sacrifices to the Modern Moloch”. For those that don’t know, Moloch was an ancient Canaanite deity to whom worshippers sacrificed their children by burning them to death on an altar. As gruesome as these lines are to write, it gives context to the extent of the anti-automobile conviction.

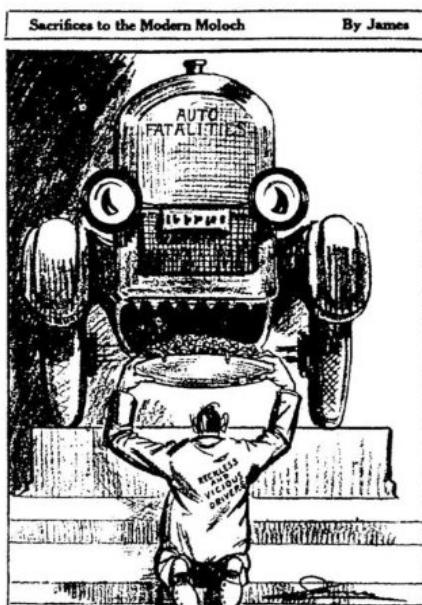


Figure 1.3

Cartoon by "James," *St. Louis Star*, November 6, 1923, p. 14.

The next piece of propaganda features the Grim Reaper plowing over innocent people. For us today this seems almost silly - not the idea of innocent people dying, but the grandiose nature of the article. Hindsight shows us that these individuals failed to see past the immediate problems with the technology rather than see its potential. In our current culture we understand vehicles are dangerous, but we also understand there is a massive benefit to technological efficiency on a worldwide scale.

NATION ROUSED AGAINST MOTOR KILLINGS

THE need for stepped up efforts to curb the alarming increase in motor vehicle fatalities was emphasized yesterday by Secretary of Commerce Herbert Hoover at a conference of state and local officials to discuss methods of combating the problem.

The conference, which opened yesterday, was called by the secretary to study the problem of the increasing number of deaths from automobile accidents. It is the second such conference to be held since the secretary established the Bureau of Motor Vehicles in the Department of Commerce in 1923. It is the first time, however, that the bureau has called such a meeting.

The bureau has been asked to recommend to the secretary measures to combat the increasing number of deaths from automobile accidents. A committee on traffic safety, composed of state and local officials, will be appointed to study the problem.

Secretary Hoover said:

Secretary Hoover's Conference Will Suggest Many Ways to Check The Alarming Increase of Automobile Fatalities.—Studying Huge Problem



In secret and state assemblies, Red Cross and other organizations, in nearly the entire country, are holding meetings to combat the problem.

"Our present position is to do all we can to help the states and cities to combat the problem," said the secretary.

"People are as yet of opinion that the automobile is a great convenience, and the public is not yet fully aware of the fact that it is a menace to the public welfare," he said.

"Therefore, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

"Finally, the bureau is doing all it can to help the states and cities to combat the problem," he said.

Those, like Henry Ford, who saw past the immediate technical shortcomings of automobiles and envisioned technologic innovation that could make them useful to the masses, benefitted most greatly. On the other hand, those who couldn't see past the flaws of these new, potentially dangerous contraptions that were noisy, expensive to fix, difficult to refuel and that lacked clear regulation around them, were the ones that trailed behind. They eventually adopted it, as everyone did, but they failed to benefit from the wave of innovation. What a waste! They lived at a critical juncture in human history and failed to see it for what it was.

The Horse & Buggy was an inferior technology and was made obsolete. The bicycle was an inferior technology but was able to carve out its own niche as a specific mode of transportation, a device for recreation and a tool for fitness. The same will be true for our current

incumbents as they are displaced by Bitcoin and blockchain. Some will be made wholly irrelevant and will cease to exist while others will carve out a niche in the future economy and serve a much narrower purpose.

The Internet

While the internet certainly had interested and established players that wanted to suppress the new technology, the most entertaining elements to analyze of the early internet antagonists were their hubris and ignorance. Computer technology has a way of baffling people in a manner that other new technologies don't. For example, contemporaries of the horse & buggy may not have seen the initial promise of the automobile, but they were able to basically understand what early cars were. They were able to see the utility of the car. But moving from analog to digital tends to give people anxiety, creates confusion, or just gives people the desire to tune out.

Although some technological revolutions are good case studies in how the establishment uses their power to suppress, the resistance to the adoption of the internet was a resistance based more upon ignorance, confusion, and an inability to see further innovation in the space. Rather than going into the various motives of the detractors of the internet, let's just look at their words. Knowing what the internet has become - being involved in nearly every element of our lives today, the punch lines kind of write themselves here.

Headline: “***The Internet? Bah!***

Hype Alert: Why cyberspace isn't, and will never be, nirvana.”

Article text:

“The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.”

By Clifford Stoll | Newsweek

Feb 27, 1995

"I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse."

Robert Metcalfe,

InfoWorld, 1995

"Most things that succeed don't require retraining 250 million people."

* discussing the need to train the next generation how to use the internet.

Waring Partridge,

Wired, 1995

"We're promised instant catalog shopping—just point and click for great deals. We'll order airline tickets over the network, make restaurant reservations and negotiate sales contracts. Stores will become obsolete. So how come my local mall does more business in an afternoon than the entire Internet handles in a month?"

Nicholas Negroponte, Director of the MIT Media Lab

Daily Mail, Tuesday, December 5, 2000

Internet 'may be just a passing fad as millions give up on it'

By James Chapman
Science Correspondent

THE Internet may be only a passing fad for many users, according to a report. Researchers found that millions were turning their back on the world wide web because of its limitations and unwilling to pay high access charges.

They say that e-mail, far from replacing other forms of communication, is leading to an overload of information.

Experts from the Virtual Society project, which produced the report, concluded that the Internet

Wesleyan director of the society said: "We've been presented with a picture of burgeoning Internet use, but there is evidence elsewhere of drop-off among younger users."

"Teenagers' use of the Internet has declined. They were energised by what you could do with it, but they've thought all that and then realised there is more to life in the real world and goes back to it."

Net loss: Two million Britons have logged off the Internet



NOW THERE'S ANOTHER
INTERNET

In a 1997 episode of 60 Minutes, interviewer Bob Simon discusses Amazon's stock price compared to Sears with a spokesperson from Amazon. Simon comments, "I think my generation grew up with Sears." To which the Amazon representative replied, "And Amazon is worth 20 percent more than Sears in terms of market capitalization." Simon chuckles at the preposterous thought and follows up with a perplexed tone as he asks, "How do you view that phenomenon where Amazon is worth more than Sears?!" ... A couple of geeks (pauses to laugh) who sketched out some software could destroy Sears Roebuck?" To which the Amazon representative simply said, "That's the beauty of technology..." The interviewer's skepticism of Amazon is difficult to understand in a time where most of Gen Z (Zoomers) and very few Millennials have never heard of Sears, much less shopped there, and conversely, Amazon is ubiquitous. But there was a time when the thought of Amazon even surviving was seen as overly bullish sentiment, let alone them becoming a multi-trillion-dollar company and their CEO becoming the world's wealthiest man.

If you have your phone or computer next to you right now, do yourself a favor and go to YouTube and type in "1994: Today Show: What is the Internet, Anyway?" It's a hilarious segment in which the anchors exhibit their utter ignorance over internet terms and even what the internet itself is. They begin the segment by discussing the "@" symbol. Bryant Gumbel correctly says that it means "at" but says that it sounds funny and he's not sure if he's right. Katie Couric then confesses that she thinks it means "about". They continue their confused conversation into the best line of the segment where Bryant Gumbel blatantly asks the question, "What is internet, anyway?" It's about a ninety second clip and it will make your day. It just goes to show how novel the internet was at that time where something as mainstream as the Today Show was even unfamiliar with it.

In a segment with Katie Couric from a different episode of the Today Show, she discusses her hesitation to adopt the internet:

"I'm afraid that if I subscribed to something like internet, I would get hooked and I would never spend time

with my family... I have no desire to be a part of the internet because I feel like I'm so inundated with information all the time that I don't want more. Don't you ever feel like it's a constant bombardment?"

The purpose of showing these quotes isn't to imply that Ms. Couric was incorrect with her assessment of the internet. In fact, she was quite right. We are constantly bombarded with information - probably even more so than she ever imagined due to our smartphones.

The point of quoting her here is to show how fragmented people think technologies will be. She says she doesn't "subscribe to the internet". At that time there were two types of people, internet users and internet abstainers. But some technologies are so pervasive that they completely change the paradigm of society. The internet is no longer just something that you log on and off from. It is the backbone of almost every element of our lives. Our news, entertainment, shopping, music, communication, social media and virtually every other aspect of our lives have been changed by the internet.

We see this same thing with Bitcoin today. There are two types of people, those who are into crypto and those who aren't. But, in the same way that the internet is integrated into all aspects of our lives, the internet of value (blockchain) will as well. Grandma probably doesn't even realize that she's using the internet when she turns on her Netflix because it looks and feels like it did when she was turning on her cable TV. This same phenomenon will happen when Grandpa goes to pay his gas bill but instead of our current financial rails, he will be sending his value via the blockchain without even knowing it.

The Bible & the Printing Press

The Roman Catholic Church was founded in an informal sense in the first century AD. For 1,500 years what it meant to be a Christian or a follower of Christ essentially meant that you were a Catholic and that the Pope was your Vicar of Christ. Vicar, meaning the mouthpiece or

voice. What the Pope said was to be interpreted as the word of God. This authority was also passed down to local Bishops and Priests.

Common folk were largely illiterate, so they relied on their Priests to read and interpret the Bible for them. The printing press was invented in 1436 by Johannes Gutenberg. Prior to that, the cost of printing a book was so incredibly high that books were limited and inaccessible to common people. Before the printing press, all the books in Europe could be counted in the thousands. Fifty years after the invention of the printing press, more than 9,000,000 books were in print⁽¹²⁾. No book benefitted more greatly from this than the Bible. It was the most printed book then and for centuries has held the title of most printed book in history.

The widespread availability of the Bible became a problem for the Catholic Church as they attempted to keep a monopoly on God's word. The Catholic Church declared producers of copies of the Bible heretics - a very serious accusation that could result in fines, imprisonment, or even torture and execution. Less than 100 years after the advent of the printing press, in 1517, Martin Luther nailed his 95 Theses to the door of the Schlosskirche Church - the proverbial first shot of the Christian Reformation. In 1521 Martin Luther was officially declared a heretic by the Pope himself. Two decades later Martin Luther got in even deeper trouble when he translated the Bible into German; the word of God was now accessible to an entirely untapped section of the world.

In the five hundred years since, Christianity has exploded around the world. The accessibility of the Bible to the average person enabled the positive influence of Christianity to seep into almost every element of our lives today. The first major hospitals, universities, and charities were founded because of Christian influence from biblical teaching. The American Constitutional Republic was founded upon the Christian ethos, largely by professing Christians. Whether one believes in its validity or not, western civilization's greatest influence is the Bible. Before the Bible could reshape humanity's morality and sense of justice, individuals literally had to face torture and execution - the most extreme resistance to any adoption of technology in history.

Airplanes, Cameras, and Netflix

Opposition to new technology is a recurring theme. Afterall, we even have entire cultures like the Amish that are devoted to a simpler, digital technology-free lifestyle. The term Luddite refers to bands of English workers that destroyed machinery they feared was threatening their jobs (1811-1816). This term is still used today and is used as a pejorative regarding those who refuse to adopt new technologies. Let's take a brief look at a few more examples of those who failed to see around corners and properly grasp the implications of innovation.

Airplanes

“There will never be such a thing as commercial aerial freighter. Freight will continue to drag its slow weight across the patient earth.”

- The Washington Post, 1909

**The first commercial freight plane took off in 1910*

The Digital Camera

Steve Sasson, a Kodak employee, invented the digital camera in 1975 and the DSLR in 1989. He pitched it to executives twice and it was declined twice. He was told that their business model was based on film. Kodak had dominated the industry since inception (130 years). They filed for bankruptcy in 2012 as the wave of digital photography made their company irrelevant.

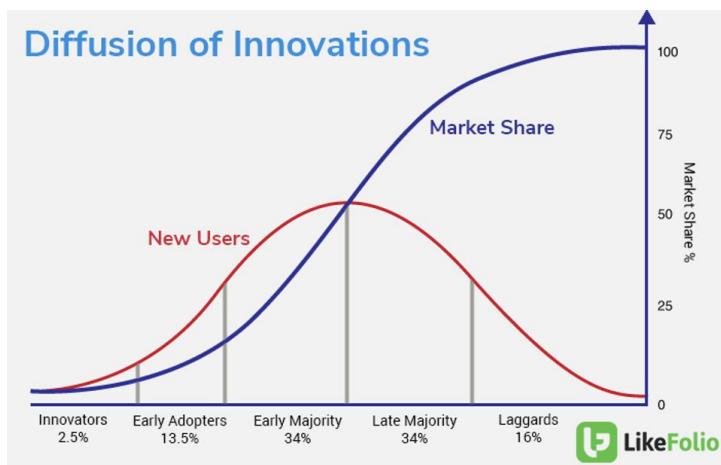
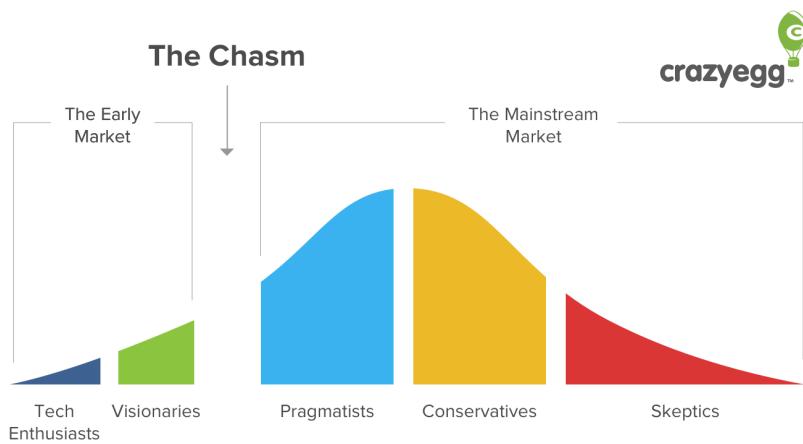
Netflix

In the year 2000, Netflix founders Reed Hastings and Marc Randolph pitched their company to Blockbuster CEO John Antioco. They told Antioco they would sell and run the online portion of Blockbuster for \$50M. Antioco flatly declined. By some accounts he

laughed them out of his office at the absurdly high price. Hastings recalls from the night after Antioco's decline: "That night, when I got into bed and closed my eyes, I had this image of all sixty thousand Blockbuster employees erupting in laughter at the ridiculousness of our proposal. Of course Antioco wasn't interested."⁽¹³⁾

In 2010 Blockbuster filed for bankruptcy. That same year Netflix hit 20M subscribers⁽¹⁴⁾. At its peak, Blockbuster was valued at \$6B. Today Netflix is valued at \$232.85B.

Let's look at the chart from the beginning of the chapter one more time and compare it to the Diffusion of Innovations chart by LikeFolio. If the bell curve in the first chart were overlaid with the bell curve of the second, it wonderfully illustrates what the market may look like upon the inevitable adoption by the conservatives and skeptics.



Taking The Orange Pill

Digital scarce assets are being adopted at a rate unlike any other technology in history. Many of those that bet against the industry in the early days have become believers. In Bitcoin, we call this “taking the Orange Pill”. Here are some of the notable skeptics turned advocates:

Michael Saylor, Founder of MicroStrategy:

Before the orange pill:

← Tweet

Michael Saylor ⚡️ 🔒 @saylor ...

#Bitcoin 💰 days are numbered. It seems like just a matter of time before it suffers the same fate as online gambling.

5:18 PM · Dec 18, 2013 · Twitter for iPad

609 Retweets 856 Quote Tweets 2,230 Likes

Reply Retweet Like Share

After the orange pill:

← Tweet

Michael Saylor ⚡️ 🔒 @saylor ...

MicroStrategy has purchased an additional 5,050 bitcoins for ~\$242.9 million in cash at an average price of ~\$48,099 per #bitcoin 💰 . As of 9/12/21 we #hodl ~114,042 bitcoins acquired for ~\$3.16 billion at an average price of ~\$27,713 per bitcoin. \$MSTR



microstrategy.com
MicroStrategy Acquires Additional 5,050 Bitcoins
September 13, 2021

Ray Dalio, Founder Bridgewater Associates (World's Largest Hedge Fund):

Before the orange pill:

"Bitcoin is a bubble... It's not an effective storehold of wealth because it has volatility to it, unlike gold."

- CNBC interview, 2017

After the orange pill:

"Personally, I'd rather have bitcoin than a bond (as an inflation hedge)."

- Forbes, May 7, 2021

"I own a little bit of bitcoin... it's almost a younger generation's alternative to gold. Bitcoin is like gold." ... he then went on to say that a prudent investor should have an allocation of bitcoin in their portfolio.

- CNBC, December 17th, 2021

Kevin O'Leary, Shark Tank Star & Mega-Entrepreneur:

Before the orange pill:

"I have no interest in being a crypto cowboy."

- CNBC, 2019

"I don't want anything to do with this crypto crap."

- CNBC, July 3rd, 2019

After the orange pill:

“My crypto holdings are now almost at 10 percent (of his total portfolio).”

- CNBC, November 11th, 2021

“I have a large stake in crypto. It makes up 20 percent of my portfolio.”

- Fox Business, March 10th, 2022

**Niall Ferguson,
world renowned Historian and Economist:**

Before the orange pill:

“Bitcoin is a delusion and has no future.”

- 2014

After the orange pill:

“We are living through a monetary revolution so multifaceted that few of us comprehend its full extent. And Bitcoin is winning it.”

- Tweet, November 29th, 2020

“A pandemic that’s contributed to rising inflation may also lead to wider cryptocurrency adoption as nervous investors look for hedges and may want to think of Bitcoin as an option on digital gold.”

- Investment Executive, October 6th, 2021

Famed Wall Street investor and billionaire Bill Miller was never on record for being anti-bitcoin but had been quiet about it for a long time. In 2021 he came out of the Bitcoin closet and publicly stated his belief in the digital asset. Even though he had spent most of 2021 speaking positively of Bitcoin, in early 2022 he shocked the world when

he revealed in an interview that he held a whopping 50 percent of his net worth in BTC.

What made these individuals shift from Bitcoin skeptics to Bitcoin believers? According to them, what made the difference was simple: information. It's the difference between ignorance and in-depth study. At one time or another they all admit to brushing off Bitcoin when they knew very little about it, but once they decided to see what the hype was all about, the light bulb went off. That's what it means to take the orange pill.

Some people are worried that new technologies will be used for nefarious purposes. This is true to some degree. New technologies can and will be used toward bad or unethical ends. Therefore, it is very important that moral people also adopt these technologies. Imagine if all the good people that wanted to uphold justice never adopted firearms and instead the only people who had them were the criminals and outlaws. There would be no way to uphold justice. It requires strength to be good - whether that strength is physical or technological. The blockchain has given individuals a Weapon of Mass Protection and is one of the few times in history that individuals have a power that enables them to resist wicked powers of any scale.

Those looking to learn about Bitcoin often get distracted and worried by the fact that there are naysayers. Especially when these naysayers are “experts” or individuals making a logical point. Yes, discourse absolutely needs to take place over these things. Blindly adopting something is foolish. Throwing the baby out with the bathwater by dismissing something new because it’s still rough around the edges is also foolish.

If someone is curious about Bitcoin, the fact that there are detractors should not be a valid enough reason to dismiss this industry. There is no historical precedent for this industry going to zero at any point in the near future so it would be most productive for dialogues about blockchain to revolve around how to make the tech better and more efficient rather than whether it’s here to stay or not - because it

emphatically is here to stay. Those already in the digital asset space who feel discomfort from the palpable tension of resistance, take comfort because this is what being early feels like.

There's no doubt that Bitcoin has faced its fair share of slander and resistance to get to this point. But it's critical to understand that this is par for the course when it comes to new tech. Bitcoin and the broader crypto industry have grown to a market capitalization in excess of \$3T with Bitcoin itself being \$1T of that. While this is an impressive and important milestone, it still has much room to grow. By comparison, the market capitalization of all gold in circulation is estimated to be \$11.489T. The market cap of the US stock market is \$93T. According to Zillow, the value of residential real estate in the US is \$33.6T.

Bitcoin and crypto will not necessarily take away value from these asset classes. Instead they will compliment them and synergistically integrate with them - substantially adding to the market capitalization of digital assets in the process. These are not mutually exclusive assets. People often think wealth must be taken from something to be put somewhere else. This isn't true. Free, fair markets and innovation have always generated exponentially more wealth.

In addition to an impressive market capitalization milestone, crypto has garnered enormous adoption from a usage perspective. In the same way that individuals in 1890 were unable to see much use for electricity beyond lighting, most people today do not see much use for crypto. But there are armies of freely associating individuals that are building an entire digital ecosystem that will be tomorrow's infrastructure for everything.

According to Brian Estes, Founder of Off the Chain Capital, for a new technology to go from 0 percent adoption to 10 percent adoption is the same amount of time that it takes to go from 10 percent to 90 percent. He goes on to focus his attention specifically on Bitcoin adoption,

“So, Bitcoin was invented in 2009. By 2019, 10 percent of US households own Bitcoin. Then last year, Brian Brooks, the Comptroller of the US Currency, mentioned that 15 percent of US households own Bitcoin. There was a survey that came out

earlier this year of 30,000 people that showed 25 percent of US households own Bitcoin.

So, we're on this mega trend of mass adoption of Bitcoin in the United States. And what this tells us, if it took 10 years to go from 0 percent to 10 percent then it's going to take 10 more years to go from 10 percent to 90 percent. So, from 2019 to 2029, in 2029 we should hit about 90 percent adoption of Bitcoin or digital wallets or some crypto assets in our portfolio. And so, this mega trend is in place and it's completely unstoppable. And you either get on board or you get run over in the next eight years. And for people that spend the time to learn what Bitcoin is... I think it would be a great benefit to them to just take 20 to 40 hours and devote to this. Understand what it is so that you can participate in this megatrend."

Blockchain and digital assets, led by Bitcoin, are being adopted at a pace unlike any other technology. From 1990 to 2000, internet users grew at an average annual pace of 63 percent. From 2010 to 2020 blockchain users have grown at an average annual rate of 113 percent⁽¹⁵⁾ - almost double the speed of the internet!

Africa is ground zero for the adoption of blockchain. Already today, Africa widely uses BTC for international remittances, banking in an otherwise unbanked region, and for protecting themselves against incredibly volatile national currencies. Several of the African currencies like the Zimbabwean dollar face inflation and volatility that are orders of magnitude greater than BTC. El Salvador has adopted BTC as a national currency. The city of Rio De Janeiro in Brazil has allocated one percent of its treasury funds to BTC as a hedge. Mayors of the biggest cities in the United States including New York and Miami are taking their paychecks in BTC. The state of Ohio allows citizens to pay their taxes in BTC.

To say that Bitcoin and crypto is going to zero or that it's a bubble will be looked back on as even more out of touch than saying the internet was a fad in the 1990s. There's a saying about upending the status quo:

“First they ignore you, then they laugh at you, then they fight you, then you win.”

In the Bitcoin community we have seen this play out. Crypto was largely ignored early on. Then later, when it was actually mentioned, it was made fun of on all the major financial shows and publications. We are currently in the fighting portion of this arc, but we are beginning to see some from the other side throwing up white flags and we are getting a taste of what this “win” will feel like. In this statement from a recent Wells Fargo report on digital assets, Wells Fargo said to its investors, (in regard to investing in cryptocurrencies)⁽¹⁶⁾

“Be patient. There is no need to rush, as most of the opportunity lies before us, not behind us.”

When I entered the crypto space, it would have seemed unfathomable to see this acknowledged by Wells Fargo, let alone published directly to their investors.

Smart money has been betting hard on Bitcoin for a significant period of time now. Adoption is happening at a breakneck pace. Those unable to see past the current inefficiencies of the tech are doomed to be like those that doubted automobiles, electricity, and the internet. They have a rationality to their skepticism and that makes them confident in their position but their rationality lacks vision. Those able to see around corners have always stood to benefit most greatly during history’s inflection points.

“People fear or cancel what they don’t understand. As soon as people start to really understand all that Bitcoin has to offer a society, my bet is that adoption will skyrocket. A truly inflation-proof asset shielded from corruption is the ultimate evolution of not only currency, but of democracy, justice, and equality for all.”

- Professor Nolan Gouveia, MBA

California Baptist University

Chapter Two: *Getting Familiar with The Terms*

“(Few saw the 2008 financial crisis coming) but there were *some* who saw it coming. While the whole world was having a big ol’ party, a few outsiders and weirdos saw what no one else could... these outsiders saw the giant lie at the heart of the economy and they saw it by doing something the rest of the suckers never thought to do: they looked.”

- *The Big Short*

Before we dive in, I would like to grant some perspective. We will be discussing large sums of money throughout the book, and I do not want the magnitude of these funds to be lost. Sometimes it’s difficult to wrap our heads around large figures - \$1M and \$1T look similar in print but are vastly different in scope.

For example, at the time of writing, Elon Musk is currently the wealthiest person in the world and his net worth is \$238B. Obviously, that’s a lot. But when you realize that even if you had made \$10,000 per day, every day, ever since the great pyramids were built that you’d still have less than seven percent of Elon’s wealth, it grants some pretty amazing perspective.

When it comes to government, we often hear about \$1T spending bills as though they are nothing. But when you realize that if you had spent \$1M every day since Jesus Christ was born that you’d only have

spent about 73 percent of a trillion dollars, it illustrates how enormous these numbers are and how real the implications.

Now let's dive in and learn about blockchain.

Glossary of Important Blockchain terms:

Blockchain

When it comes to buzzwords in popular culture, “blockchain” is certainly one of them, especially in business and finance. Many people who aspire to become very wealthy in a short period of time no matter what their background is or what type of popular culture they are into - professional football, Hollywood, hip hop, politics, or economics - are intrigued by blockchain. Viewing this industry as a “get rich quick scheme” is a misguided one. To separate yourself from the madness of the crowds, it’s important to understand what blockchain actually is.

In a nutshell, all financial systems that have ever existed required middlemen. The advent of blockchain technology has enabled financial systems that do not require a middleman. The importance of this cannot be overstated, so much of the remainder of this book will be devoted to making this case.

This new technology isn’t a device to get rich quick from because blockchain, in and of itself, is just a new accounting system. It’s the applications built on top of blockchain that allow individuals to participate in one of the greatest wealth transfers in history. This transfer will not happen overnight, but it will happen much more quickly than most people expect. More on that in later chapters.

Key Point: “In a nutshell, all financial systems that have ever existed required middlemen. However, with the innovation of blockchain technology, financial systems no longer require a middleman.”

Bitcoin and blockchain are two separate things. Bitcoin is the unit of account or the currency of the Bitcoin Blockchain. The protocol,

or blockchain named Bitcoin, is represented with a capital “B” and bitcoin, the currency, is preceded with a lowercase “b” or, written as “BTC”. The blockchain is the decentralized ledger system that enables the network to function and embody the characteristics that make it special - attributes we will discuss shortly. Think of it in this very simplistic way: the internet was once a new technology and email was the first killer application built on top of it. In 2009, blockchain was the new technology and Bitcoin was the first app built on it. They happened to be created at the same time, by the same person, but it may be helpful to envision them as two separate inventions, with one being built on top of the other.

A broad understanding of blockchain simply put is that it is a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across multiple computers (tens of thousands of anonymous computers around the world). These are also known as nodes. One of the truly revolutionary elements of this is that it allows users to be linked peer-to-peer, for the first time ever. No other monetary system has wanted to or had the capability of connecting individuals directly, without a middleman. Incentives made it quite lucrative to be said middleman. Historically this meant you could develop the equivalent of a multi-million or even multi-billion-dollar business; think Visa and Mastercard. The blockchain is a ledger that anyone may use at any time. It cannot discriminate. It cannot pick winners and losers. There are currently well over 100 million users on the Bitcoin Blockchain, and that number grows dramatically every day.

Allow me to give you a more technical and hopefully still accessible understanding of the blockchain in regard to how it works. It is called a block-chain because every 10 minutes a new block of transactions is added to the chain. This chain is the history of all the blocks that came before it. Once a set of transactions (a block) has been added to the chain, it is sealed and can never be altered. This harkens to the term you often hear within the blockchain space: *immutable*. Blockchain’s immutability gives it a broad appeal. This aspect is one more way that demonstrates blockchain cannot be controlled by the wealthy or mighty. No matter how rich or powerful someone is, they are no more capable of changing past blocks than you or I. It cannot be

changed by users of the network, miners, governments, hackers, no one - making it a highly reliable record. In fact, nothing like it has ever existed before.

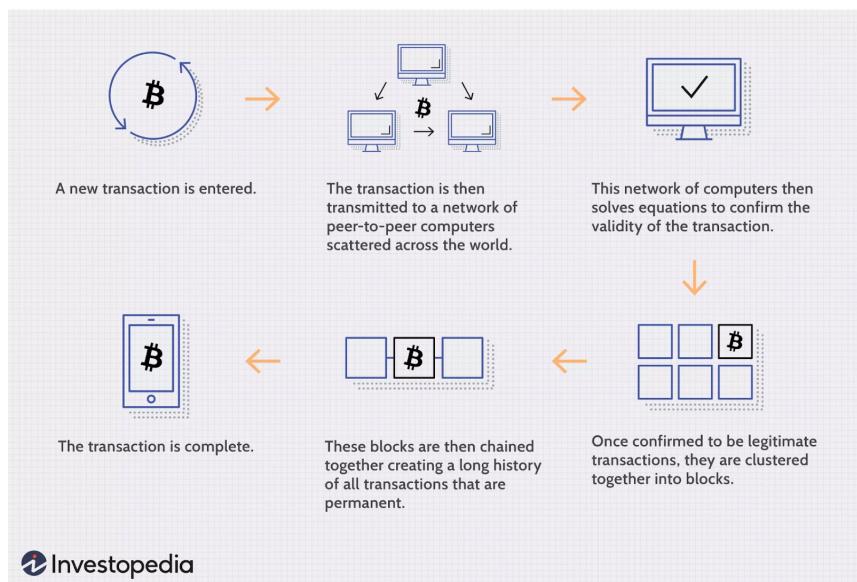
In stark contrast to our current financial systems, the blockchain is quite transparent. Imagine an Excel spreadsheet on the cloud that shows all the financial transactions in the world. Everyone has access to view that spreadsheet at any time. For there to be an open financial system, transparency is essential. This protects the network from being controlled by any one individual or group by obfuscating transactions, censoring transactions or even somehow erasing payment histories.

You may be thinking, “I don’t want people to be able to see all of my transactions!” Don’t worry, the record essentially just shows that Wallet A sent X amount of bitcoin to Wallet B. Because these wallets are cryptographically protected, no one has access to your wallet, nor do they know who owns the wallet. This transparency serves as one of the security measures of the blockchain because all nodes on the network perform a full and complete audit of the entire network history every 10 minutes. This ensures fairness and accurate accounting unlike any set of books in history.

Within the cryptocurrency space you may also hear the term “distributed ledger technology”. Blockchain is the first and most widely used form of distributed ledger technology. But it’s worth noting that there are other forms including: Tangle, Gossip, Directed Acyclic Graph, Holochain DLT, and Tempo. While we will not touch on the individual merits of these, they are attempting to solve the inefficiencies of blockchain, mostly in terms of speed. But this inherently makes them less secure, at least in their current iterations. Blockchain gets the spotlight because it has been proven worthy to secure trillions of dollars of value and the Bitcoin blockchain specifically has proven thus far to be unhackable. While these other distributed ledgers are very much theoretical, blockchain has over a decade of high value real world implementation.

Note: Distributed and decentralized are two very different things. You may hear people use them

interchangeably but please be aware that they are not the same thing. Distributed means that everyone can see a copy of the ledger but only a central party has control over what goes on the ledger. Decentralized means that what goes on the ledger is controlled by a decentralized consensus. It's the difference between a king (distributed) and a republic (decentralized).



 Investopedia

(48)

Chart courtesy of Investopedia

Satoshi Nakamoto

Satoshi Nakamoto is the pseudonymous creator of Bitcoin. The public does not know who Satoshi is - this was a strategic move and exhibits the brilliance of Bitcoin's creator. Critics will say that Satoshi obfuscated his identity because he was afraid the authorities would come after him. While this may be true to some degree, I don't think this is entirely the reason because his creation was not illegal at its conception, and over a decade later it still isn't.

I believe Satoshi Nakamoto hid his identity so critics of Bitcoin would have to argue against its merits rather than the merits of an individual - as all individuals are flawed and can be disparaged. I mean, just look at what happens to beloved public figures when they spend decades in public life being adored and admired only to be put under a microscope and slandered when they run for political office. Satoshi knew that allowing Bitcoin to stand on its own and handing it over to the people was the best path forward. This act can be viewed similarly to how George Washington abdicated the chance at authoritarian power after America's Revolutionary War and instead advocated for a decentralization of power via America's Constitutional Republic.

It is possible, even probable, that Satoshi Nakamoto isn't just a single individual. The scope of thought and brilliance of Bitcoin seems to have required the cumulative ability of a cohort of great minds. It may even be correct to refer to Satoshi Nakamoto as a woman. But I will refer to Satoshi as a singular male throughout this book because that is the way he presented himself through the earliest stages of Bitcoin on forums and in email conversations.

To further add to the great mystery of Bitcoin's creator, on April 26th, 2011, Satoshi responded to an email from a Bitcoin community member named Gavin Andresen:

"I wish you wouldn't keep talking about me as a mysterious shadowy figure, the press just turns that into a pirate currency angle. Maybe instead make it about the open-source project and give more credit to your dev contributors; it helps motivate them.."

On that same day Satoshi responded to an email from another early Bitcoin developer, Mike Hearn:

"I've moved on to other things and probably won't be around in the future."

And he was never heard from again.

Satoshi Nakamoto was a brilliant programmer and visionary but may not have been a great marketer. Marketing 101 requires that in promoting something, you need to make it easily understood by your audience. Aside from the complexities of Bitcoin as a robust technology, its two components bear the same name: bitcoin is a digital currency, but Bitcoin is also the monetary network.

We tend to refer to these two distinct things as one, but it's helpful to articulate the difference. To better understand the distinctions, let's look at how our current monetary system works: United States Dollars are the currency and Visa, for example, is the monetary network. In this instance, it's very easy to see that you send dollars across the Visa payment rails from Person A to Person B. You don't send visa bucks over the Visa network. But, when we refer to Bitcoin, we send bitcoin cryptocurrency across Bitcoin payment rails from Person A to Person B. Sounds a bit redundant, right? Understanding this distinction will help you better understand the nuances of how the system works going forward.

Some Bitcoin skeptics have a hard time with the idea of a pseudonymous founder that is no longer around. They do not value the fact that the problem with most entities is the people rather than the systems or processes of the entity. Think about it, when someone complains about the government, they are complaining about a bad politician. They are typically not complaining about the constitution or the checks and balances system. If you can remove the people and address the system based on its own merits, there is real power in that. In fact, this is unlike any system we have ever seen before. Have we ever questioned who created the convection oven, or who invented the jet engine? Probably not, but we use them anyway, not because of who their creator was, but because they work.

It is unknown if Satoshi Nakamoto will ever resurface, but it seems quite evident that he will not. Interestingly, the wallets assumed to be his, collectively hold one million BTC and have also been dormant since he disappeared. We can have some inclination that these are his wallets because they are the wallets where the earliest mined BTC coins went. His one million coins are obviously no small sum as the dollar value of these coins are in excess of \$65 billion at the time of writing -

making Satoshi among the wealthiest people on planet Earth. Imagine if the world's first trillionaire is a pseudonymous computer programmer who chose to vanish so Bitcoin could have no central figure. Deciding to forego his fortune so he could gift the world its first decentralized, fair and just monetary network! Nakamoto reaches the unprecedented trillionaire status when BTC's value crosses \$1 million per coin.

Satoshi/Sat

The Bitcoin community named the smallest unit of Bitcoin a "Satoshi" or "Sat". In the same way that a US Dollar is divisible down to \$0.01, a Bitcoin is divisible down to 0.00000001. While one hundred pennies are the equivalent of a single US Dollar, it takes one hundred million Sats to equal a single BTC. We will get into bitcoin's highly divisible nature in an upcoming section. Rest assured that this divisibility was intentional. If BTC attains its goal of becoming a global currency, everyday items will not be priced in full bitcoin, they will be priced in Sats.

Satoshi's Value



coinc Telegraph.com | (47)

Chart courtesy of Cointelegraph

Mining

Imagine you are attempting to create a decentralized community of computers (all people that may or may not even know one another) to validate transactions and you're relying on these individuals to volunteer their computing resources (ie: electricity cost, hardware cost, etc.) to secure the network, how would you do that? Maybe some people will idealistically believe in your mission and perhaps freely volunteer their resources. As much as we would like to think the best of people, you probably wouldn't generate much interest; if you don't have many nodes (people with computers) on that network, it might be somewhat decentralized, but it wouldn't be very big or strong. If your goal is to transfer money or value over that network, then you must ensure that it's as strong as possible by having as many nodes as possible and therefore you must offer appropriate incentives for those who will secure the network.

This is where another stroke of genius is presented by Satoshi Nakamoto. Blockchain, like Capitalism, benefits all participants by assuming that said participants will act in their own self-interest. So, if you need individuals with computers to secure your network and you don't know who they are, and they don't know who you are (this is known as the Byzantine Generals Problem in computer science), then the way to incentivize them is to have the network generate coins and pay those volunteers to process transactions and secure the network. The participants lending their computing power to the network are called Miners, and they create consensus with the other nodes on the network via something called Proof of Work (PoW) - this simply means that a computer that is mining bitcoin can *prove* it contributed computing power (work) to the network.

Allow me to elaborate. The Bitcoin algorithm is pre-programmed to require miners to produce a new block of transactions every 10 minutes. Miners will race to solve a computational puzzle and whichever miner solves it first, gets to put the next block into the chain and when they do so, they are rewarded with bitcoin. By solving this puzzle, the miner proves to everyone else in the community that they provided a large amount of computational work to help secure the network - this is

where the “work” in *Proof of Work* (PoW) comes from. At the time of writing, the miners are rewarded with 6.25 bitcoin every 10 minutes.

Individuals can buy, sell, and hold bitcoin without ever mining. Mining is not required to participate in the Bitcoin network. But, for those that do mine bitcoin, they are rewarded. These rewards started out relatively insignificant, but they have grown so substantially that an industry has emerged and now there are publicly traded companies that have warehouses full of bitcoin-specific mining computers. But anyone can be a bitcoin miner. College students mine bitcoin from their dorm rooms, billion-dollar companies mine it near cheap and renewable energy sources, and now even countries mine bitcoin in the same way that Saudi Arabia produces oil as a domestic commodity.

Bitcoin mining is a very interesting and deep topic, and we will dive further into questions around its environmental impact, how the *computational puzzle* miners must solve works, and more in the “Short Answers to Common Questions” section later in the book.

Returning to the brilliance of Nakamoto’s solution to the Byzantine Generals Problem: this solution is derived from aligning the interests of everyone involved. There are entire fields of economics that study incentive structures within society and how to best align the goals of individuals. Nakamoto developed a system where the self-serving actions of anyone on the network have some sort of positive effect for others on the network. In the same way that a bee is only concerned with drinking nectar and unintentionally pollinates the flowers that it drinks from, so too do actors on Bitcoin benefit others. For example, a miner that desires to extract the most value from the network to enrich herself with bitcoin block rewards will use her computing power to do so. This computing power further secures the network for all other users. Her pursuit of profit benefits other people.

This is even true for Bitcoin with things that are not directly part of the network. This book you are reading right now is being written by someone with a deep conviction about this technology and is contributing hundreds of hours of study, writing, editing, and promotion so that more people will know about Bitcoin and it will grow further. Maybe I’ll even sell a bunch of books and get rich. While that is highly unlikely, the growth of the network or me selling a bunch of books

means more acceptance of the asset that I hold, and it benefits me. By learning about it, it will also benefit you. When the network grows, all other nodes on the network benefit as well. People in China, Brazil, Japan, and Europe that hold bitcoin benefit from the work of that miner who is trying to enrich herself; they benefit from the long hours of work I have done to develop this book. The only thing we can ever really count on is people's self-interest - this is part of what makes Bitcoin so unbreakable: the alignment of everyone's self-interest.



Mining farms are operations solely focused on earning BTC rewards. In doing so, they provide security to the network.

Encryption

Imagine it's the 1700s and you want to send a note to your friend. The contents of the note are very important as they give instructions for how to find your fortune in the event that you die. You are not totally sure that you can trust your mail carrier. Even if you seal the letter, he could open it and use the instructions to find your treasure.

Even if your mail carrier is honest, he might get robbed along the way, and you just can't leave your fortune up to that kind of chance.

So, it begs the question, how do you send a sensitive message and be sure the contents will not be read by other people? For thousands of years the answer has been encryption. That's right, the key component in blockchain and cryptocurrencies is a technology that has been around for millenia.

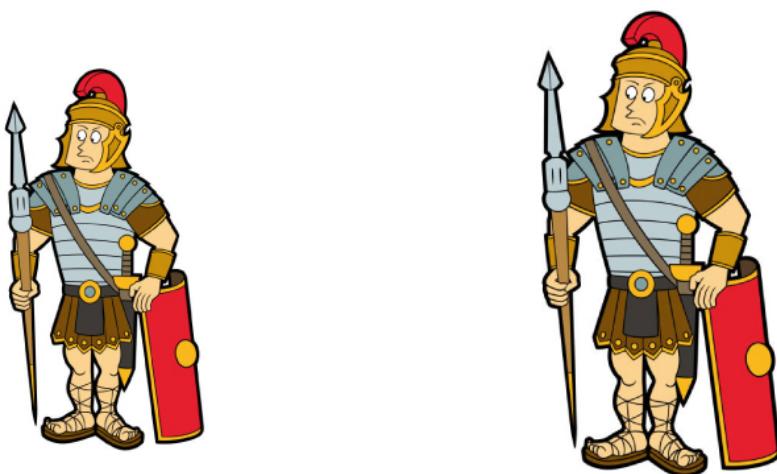
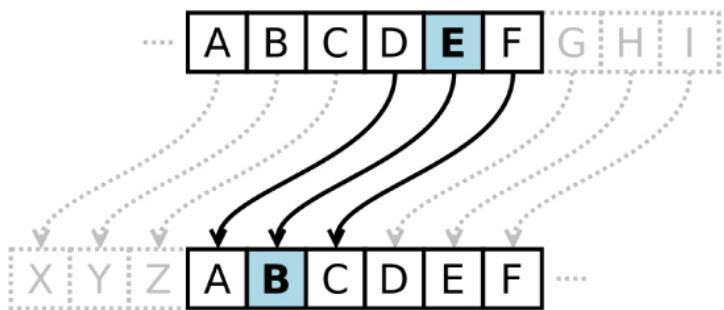
In a really basic form, here's how encryption works: Person A sends an encrypted message, which essentially means that it's a scrambled form of the original message. Both Person A and Person B will share the cipher with one another, which is like the key to unlock the scrambled message. A famous ancient cipher of the Roman legions was called the Caesar Cipher. This was a simple cipher that took the original message and just shifted each letter three spaces backwards in the alphabet. This was a rudimentary way for Roman messengers to send sensitive messages and battle plans across long distances where they could be resistant to interception by the enemy.

Bitcoin wallets are where one stores their BTC. These wallets use encryption technology to protect the wallet holder's property. Bitcoin wallets are very different from a traditional bank account. With a traditional bank account, the bank holds your funds. You must request permission from the bank to access your funds. Banks have rules and regulations that you must follow, though this is typically not a huge issue for most individuals. It can become a problem if you want to withdraw more than \$10,000. If you have ever attempted to withdraw more than \$10,000 from your bank account, you will quickly realize that you are not totally sovereign over your own money.

Bitcoin wallets are quite different from bank accounts because no one other than you controls or has access to your funds. Encryption provides incredibly sophisticated security to enable an individual to store large amounts of value within otherwise simple looking software on a phone, computer or other storage device. This encryption process means that each BTC wallet has two addresses, a public and private address. We will cover both of these in the following sections.



The Caesar Cipher



“TB XQQXZH XQ AXTK!”

“We attack at dawn!”

Public key = you can show this to anyone.

A public key is also known as a public address. Going back to our earlier example of Wallet A sending X amount of BTC to Wallet B; Wallet A would have a string of numbers and letters that represent it on the Bitcoin ledger. So, in this example, Wallet A would look something like this: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Your public key/address is like your email address - it really doesn't matter who knows it because they can only send to it. The public key cannot be used to withdraw BTC.

Private Key

Private key = DO NOT show this to anyone.

Your private key is some serious business. You don't mess around with your private key. Only you should have access to this key. It's the cipher that we talked about a couple of sections ago. It should be stored in a highly secure way, typically in multiple secure locations in case something unforeseen happens. It's like a physical key in the sense that you can make copies of it and store it in various locations.

If your public key is like your email address, then your private key would be like your password - you would never give it out because then people could send out emails. And you don't want people to send out your BTC. Bitcoin uses an algorithm called SHA-256. That sounds nerdy and technical but in a nutshell that means that your private key is a 256 character string. It is highly cryptographically secure.

If you are using a service like Coinbase, Binance, or some other exchange or custodian service, you will not have access to your private key. These services provided by centralized companies are a great option for getting started with BTC, though. Self-custody can be a somewhat intimidating endeavor for many people, so starting off by holding small amounts of BTC on an exchange is perfectly understandable. Just keep in mind that one should eventually move toward self-custody as holding crypto assets on an exchange kind of goes against the ethos of Bitcoin. One of the highest principles of crypto is the concept of self-sovereignty - the ability to hold your own money. It can be well-argued that unless

you are the only person with the private key, you don't truly own your BTC. This is because whomever else has the private key has equal access to those funds.

There is a well-known saying in the crypto universe: "Not your keys, not your crypto." I'm personally fond of the more lay person adaptation of this saying coined by Isaiah Jackson in his book *Bitcoin and Black America*: "Not yo' keys, not yo' cheese!"

One may not feel comfortable with maintaining their own private key right away. If this is the case, then an exchange platform that offers a custodial option such as Coinbase, PayPal, Cash App, or Robinhood is useful. They make accessibility easier for those new to Bitcoin. But, as your knowledge of the space grows and your funds become a more material value, it becomes prudent to custody them yourself.

Hot vs. Cold Storage

Now that we properly understand public and private keys, and we know how critical it is to secure our private keys, it is vitally important to understand the various methods of storage. This is actually quite simple. Hot storage is a Bitcoin wallet that you simply download to your computer or device that allows you to send or receive BTC and stores your private keys. These devices are connected to the internet or any other type of public or local network.

Common forms of hot storage could be something like a wallet on your smartphone or a wallet on an exchange such as Coinbase. This is an efficient method of storage for a small amount of funds that are easily accessible for purchases. Think of this like having cash in your wallet. You may have enough to buy some meals, gas, or groceries, but you wouldn't keep enough cash with you to buy a car. Hot storage is quickly accessible for the user but has the inherent risk of potentially being accessible to bad actors through the internet, similar to the vulnerabilities of your online bank account.

Cold storage is like your savings account where you keep the bulk of your money. It's called cold storage because it is stored on hardware that is not connected to the internet. There are also such things as *paper wallets* in crypto, which are a very secure form of cold storage.

This is where you write down your private key or seed phrase by hand on a piece of paper. This means that even if your hardware had a keyboard reader malware that recorded your keystrokes, it wouldn't be able to detect anything. There would be no electronic record of your private key being generated and it would be stored entirely offline. Cold storage is commonly done with devices called *hardware wallets*. Ledger and Trezor are popular and reliable hardware wallet manufacturers.

As a user of Bitcoin and other cryptocurrencies, it's important to understand when it is appropriate to use hot storage vs cold storage to limit your vulnerability. This might sound daunting or stressful to new users, but it comes with the territory - Bitcoin is revolutionary because of the fact that individuals can hold large amounts of their wealth digitally in a secure way for the first time. While this might sound like a lot of work when reading about it, I assure you that in practice, it is actually quite simple. Having complete sovereignty over your money is pretty incredible. Try accessing your funds via your bank on a Sunday afternoon - it won't happen. With your hot and cold storage, you can access your money at any time for any reason.

Halving/Halvening

The Bitcoin community still has not officially decided whether the event that happens every four years is called the “halving” or a “halvening”. Regardless, what this refers to is that every four years the amount of bitcoin awarded to miners for each block gets cut in half. When Bitcoin started in 2009, the reward every 10 minutes was 50 bitcoin. When the first halving took place on November 28th, 2012, the block reward was cut down to 25 bitcoin.

This process continues about every four years. In Bitcoin's early years the inflation rate of its flow (incoming supply) was relatively high. This was intentional because unless there were plenty of coins in circulation, people would have been less likely to encounter BTC at all. Imagine if there was only one bitcoin. What are the chances that anyone would have even heard of it, let alone owned it? The early high inflation rate can be thought of as a growth strategy so that early adopters are rewarded and will then be incentivized to improve and market the

network. The stock to flow ratio of bitcoin is already quite high and will be higher than gold's after the 2024 halving - meaning that the amount of new bitcoin relative to how many are already in circulation will be a small amount - a pretty shocking feat since gold has a five-thousand-year history while Bitcoin will have accomplished this in only sixteen years. I believe that the 2024 halving will be one of the biggest inflection points for explosive price growth in BTC because it will mark BTC as one of the scarcest assets on the planet while hitting a quantum leap forward in adoption and real-world utility.

The reason you hear people say “about every four years” regarding the halving cycle is because it’s not actually based on time; the halving occurs every 210,000 blocks. Since blocks are produced about every 10 minutes, this equates to approximately four years.

I believe that Satoshi Nakamoto was an avid reader of renowned economist Milton Friedman, in part, because of Nakamoto’s implementation of the halving cycle. In Friedman’s famous book *Capitalism and Freedom* (1962) he surveyed various monetary systems of the past and concluded from his empirical analysis that the best monetary system would be one with a predictable supply of new money.

“In the present state of our knowledge, it seems to me desirable to state the rule in terms of the behavior of the stock of money. My choice at the moment would be a legislated rule instructing the monetary authority to achieve a specified rate of growth in the stock of money.”

Because Friedman was unable to foresee the advent of Bitcoin, he had to default to hoping for reasonable legislation on the matter of currency supply. But that is obviously flawed because it relies on individuals, and individuals in positions of power have shown they are susceptible to corruption and fallibility time and time again. Friedman went on to articulate what a reasonable incoming money supply should look like:

“I would specify that the Reserve System shall see to it that the total stock of money so defined rises month by month, and indeed, so far as possible, day by day, at an annual rate of X percent, where X is some number between 3 and 5. The precise definition of money adopted, or the precise rate of growth chosen, makes far less difference than the definite choice of a particular definition and a particular rate of growth.”

To Friedman, money supply was of the utmost importance to a healthy financial system. The proper solution to his concern is an algorithmic monetary system where the rules dictating the money supply are clearly defined. The halving fits this definition perfectly. It's almost as if Milton Friedman is describing Bitcoin in his writings. I imagine if he were still alive today, he would be a strong advocate of Bitcoin for its free-market principles and specifically here, its programmatic money supply.

Fiat systems tend toward drastically or even parabolically increasing their currency supply over time. The Bitcoin halving schedule ensures that high inflation was present to start the network to get coins into the hands of network participants, but as time goes on, the inflation rate gets halved - the literal opposite of exponential growth. To understand the power of a supply that gets cut in half, it first helps to understand the power of exponential growth.

There was once a prince in India who was a chess enthusiast and had the habit of challenging wise visitors to a game of chess. One day a traveling sage was challenged by the prince. The sage, having played this game all his life with some of the cleverest people from all over the world gladly accepted the prince's challenge. To motivate his

opponent, the prince offered any reward that the sage could name. The sage modestly asked just for a few grains of rice in the following manner: the prince was to put a single grain of rice on the first chess square and double it on every consequent one. The prince accepted the sage's request.

Having lost the game and being a man of his word, the prince ordered a bag of rice to be brought to the chess board. Then he started placing rice grains according to the arrangement: 1 grain on the first square, 2 on the second, 4 on the third, 8 on the fourth and so on.

Following the exponential growth of the rice payment, the prince quickly realized that he was unable to fulfill his promise because on the twentieth square he would have to put 1,000,000 grains of rice. On the fortieth square, the prince would have to put 1,000,000,000 grains of rice. And, finally, on the sixty-fourth square, the prince would have had to put more than 18,000,000,000,000,000 grains of rice which is equal to about 210 billion tons - sufficient enough to cover the entirety of the prince's territory with a meter thick layer of rice.

At that point the sage told the prince he doesn't have to pay the debt immediately but could do so over time. And so, the sage became the wealthiest person in the world.

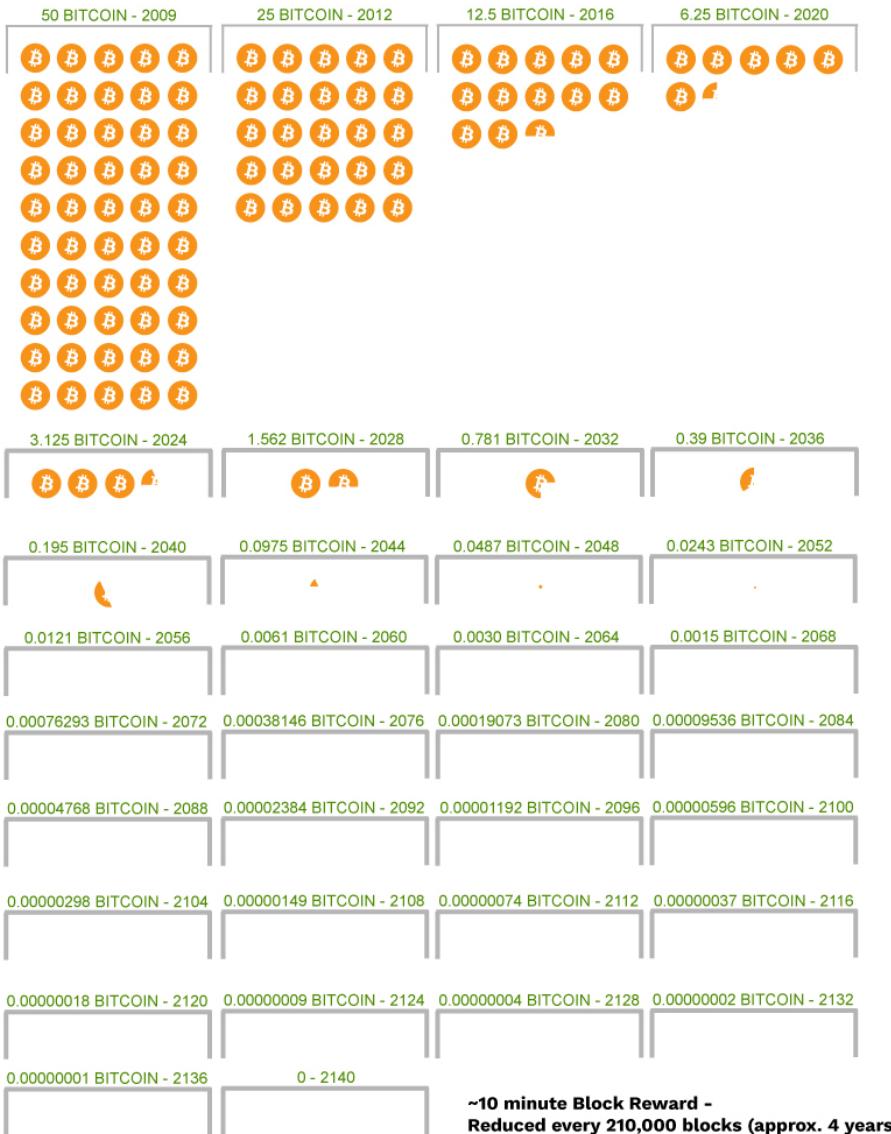
Exponential growth is a pretty amazing thing as we will also discuss in later sections. As drastic as exponential growth is, diminishing something by halving is equally powerful. This is illustrated in the supply of bitcoin. The first bitcoin were mined on January 3rd, 2009. As these lines are written in November 2021 there have been 18,875,825 bitcoin mined. In the first thirteen years of Bitcoin's existence, 90 percent of bitcoin have been mined. It is estimated that the final pieces of bitcoin

will be mined in February 2140. That's right, because the incoming supply of bitcoin is cut in half every four years, the first 90 percent of coins will be produced in thirteen years and the final 10 percent will be produced over the next one hundred and nineteen years! The first 18,875,825 are already in circulation and the final 2,124,175 will take over a century to be produced. Astonishing.

The monetary policy and foresight of Satoshi Nakamoto, as demonstrated in bitcoin's limited supply and minting schedule, was absolutely brilliant.



Bitcoin Halving Schedule



Stock to Flow Ratio

Use of the Stock to Flow Ratio (S2F) has been widely used for decades to assess the current value and the projected change in value of natural resources and precious commodities like gold and silver. It measures the current *stock* of an asset against the *flow* of new production by how much is mined in a year. A higher ratio indicates more scarcity (high stock to low flow), which in turn indicates a higher future value. A low ratio indicates a large incoming flow of newly produced assets vs a relatively small current stock.

S2F is not generally applied to currencies like the US dollar, but for argument's sake, if you were to apply it in the year 2020, the US dollar would have a dramatically low S2F ratio (meaning a high volume of new currency was printed relative to the existing supply). Depending on the metric, currency supply in the United States increased anywhere from 20-40 percent in that one year. But, even if you take the lower number, USD has a very low S2F, making it a very abundant or common asset.

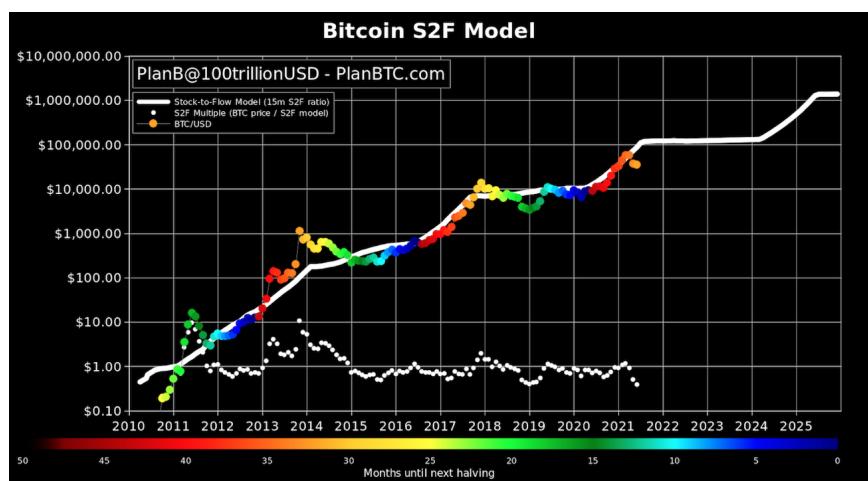
According to the general principle of supply and demand, this should trigger a significant value decrease in the US dollar, also known as inflation.

Furthermore, S2F is used with respect to commodities like gold because they have a somewhat predictable schedule of new production. We can have a rough estimate of how many gold mines exist around the world and about what rate they mine at. This factor is an inherent weakness in fiat currencies because there is no guarantee of a pace of future scheduled production.

This is where bitcoin has a tremendous advantage. While gold and silver have the most predictable models for S2F, there are still no guarantees. We don't know exactly how much gold has been mined. We don't know exactly how much gold has been released to the market vs how much has been hoarded by the miners, governments, or collectors. Additionally, if the price of gold goes up, gold miners will be incentivized to either sell some of their hoarded gold reserves or mine more out of the ground, thus increasing the supply and suppressing the price through a market equilibrium.

Bitcoin is the world's first programmatic money so we know with a surgical precision how much incoming supply there will be at any given time. One could even pick a date one hundred years in the future and be able to accurately estimate how much bitcoin will be in circulation - we have never seen anything like this before! Unlike gold, which can be mined more as its price goes up, bitcoin cannot be mined at a faster pace, no matter how much its price goes up. A set amount of bitcoin will always be mined every ten minutes, regardless of how much demand there is for it. Any additional mining capacity will not mine more bitcoin, it will just increase the security and the decentralization of the network.

In 2019 use of S2F on BTC became popularized by a famous pseudonymous chartist called Plan B. He has used the model to predict price levels retrospectively and prospectively with a high level of accuracy. Plan B's S2F model predicts a \$1,000,000 bitcoin price by 2025. While this chart has been historically accurate, we will have to wait and see about the future validity of this model.





USD vs BTC Stock to Flow

*for the year 2020

USD vs Bitcoin



Supply as of
January 1st, 2020

\$15,500,000,000,000

—
New production in
2020

\$3,340,000,000,000
(21.5%)

S2F = Low

Supply as of
January 1st, 2020

18,190,000

—
New production in
2020

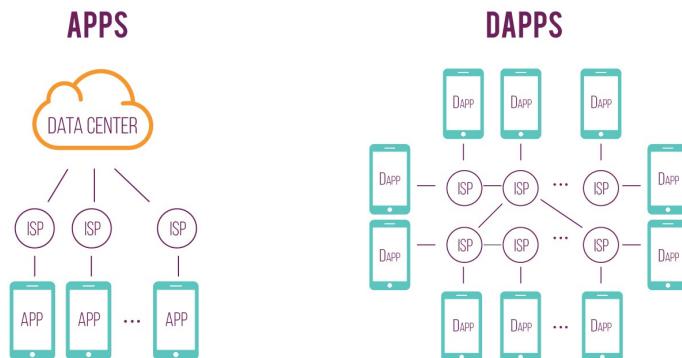
400,000
(2%)

S2F = High

dApps

dApp is the cool abbreviation for the term *decentralized application*. dApps are enabled by protocols that run *smart contracts*. We will touch more on smart contracts throughout this book, but for now, it's just important to know that smart contract platforms like Ethereum are what make dApps and other new decentralized tools possible. If Bitcoin is like Apple Pay, then Ethereum would be like the App Store. One is for sending value while the other is for building things. While this book is titled *Bitcoin Evangelism*, it should be noted that Ethereum and other smart contract platforms will play a pivotal role in our decentralized future.

To understand what a decentralized application is, it is helpful to define what a regular, or *centralized application* is. Facebook is a very popular application for any device, as you already know. Facebook provides tremendous value for their users by plugging them into a worldwide social network. In exchange, users pay with their data, privacy, and efficiency at work - something many of us shockingly have little issue giving up. I digress. All the servers, hardware, software, maintenance, and everything else that goes into making this network available to users is provided by a central entity - Facebook and its parent company Meta.



Source: towardsdatascience.com/what-is-a-dapp-a455ac5f7def

They incur absolutely massive expenses to do so, but in return, they receive even greater compensation. They create the rules and can

change them as they please. They have full control over the network and how users can interact with it. In addition to users paying with their privacy, users also generate revenue for Facebook by viewing ads. This is an age-old practice and there is nothing ethically wrong with it. But, as we will see with dApps, there are some pretty cool technological advancements when it comes to how users interact with ads.

In stark contrast, dApps are applications where many individuals and/or groups loosely collaborate to provide everything necessary for the application to function. In the case of Facebook's decentralized counterpart dAppBook (not real), all the programming, servers, and other necessary items for the network to function would be provided by these distinctly separate entities or people that share a common goal of providing this decentralized alternative to Facebook. Using the power of cryptography, they can offer users a platform that protects their information, even from the dApp node validators themselves. With cryptographic data privacy, some dApps even have the ability to make it so that users get paid directly by advertisers to be shown ads, if they opt to even be advertised to at all. If Bitcoin provides the ability to have sovereignty over one's own money, dApps may indeed be able to provide sovereignty over one's own data.

dApp developers are typically willing to contribute to the network for a philosophical reason and/or because these applications have ways of providing economic incentives for those that do so. We won't go further into those incentives or even specifically how dApps work here, but you can be quite certain that dApps will change the face of how the world operates in the very near future, so further study is certainly warranted.

We only briefly touched on what a smart contract is so you may be wondering why a smart contract would be needed in a dApp. You can think of a smart contract as the set of rules for a dApp. For example, if you had a centralized gambling app you could quickly see the inherent problems. Why would the creators of that gambling app play fair? How would you know if they are giving you traditional casino odds, or if they are cheating you? You wouldn't. This is where a dApp using a smart contract would come in. The smart contract would have the rules and odds of the game written into it for everyone to see. If the player (Wallet

A) wins a hand of blackjack, then the house (Wallet B) pays Wallet A the appropriate amount. The player does not have to trust that the house is playing fair because they can verify for themselves at any time by reading the smart contract.

The next generation of entrepreneurs and innovators are looking at existing businesses and thinking of all sorts of ways in which this new technology can be a paradigm shift for traditional models. Look at a business like Uber. What good or service do they provide? They simply match drivers and riders via a clean working interface. It's been an incredibly helpful and convenient service to many. But that same service can be provided by a smart contract and run on Ethereum.

Think of the fiscal implications. If Uber takes a 25 percent cut of every transaction and now Uber is no longer needed, miners of the token (those that process the transactions) can get paid in mining rewards without taking a portion of the fare. This could create a competitive free market for drivers. In fact, these drivers would essentially be entrepreneurs, running their own business of providing rides and charging their own rates. They could lower their rates by 15 percent and still make 10 percent more than they were making while working with Uber. As any prudent business person knows, when you lower your prices, demand goes up. So, drivers would be able to make 10 percent more per fare while making it more economically feasible for riders - creating greater demand at a higher profit margin. More business at higher margins sounds good to me. I expect that ten years from now many existing businesses will be disrupted by dApp services and DAO's (which we will touch on later). dApps may even make every worker in the gig economy into a true entrepreneur, using an algorithm to match the services they provide with prospective customers.

Fiat currency

Fiat currency has nothing to do with the car company. Yet, as a playful joke, on August 2nd, 2018, the car company Fiat, Tweeted: "Why do these 'cryptocurrency' people hate us so much? Leave us alone." The tweet was prompted by the reality that "crypto people" generally dislike

fiat and had been vigorously tweeting nasty things with #Fiat at the end of them.

Fiat currency is what every government currency on the face of the earth is. This currency is not backed by any kind of commodity like gold (as they used to be) but instead it is backed “by decree”. What does that mean? It literally means that it has value because the government says it does. It is given some additional value by the fact that every government requires its citizens to pay taxes in their sovereign currency - thus creating some demand for it. Lastly, it has some value if it is widely accepted. In the same way that we say Bitcoin has a network effect, a fiat



currency like USD has this network effect as well since it is very widely accepted around the world and enables one to transact in most places. But fiat currency contains a weakness in that there is nothing to restrain governments from printing more at their whim, thereby weakening its value (inflation) when it is not backed by a commodity like gold. Modern Monetary Theorists (the academics that make big government spenders feel like they are smart) suggest that economies can be stimulated into perpetual growth by ensuring capital is consistently injected into the system to create demand. Historically, this has had a 100 percent failure rate but MMT proponents argue “it is different this time.” To me, that is not a compelling argument, especially since we can study cases of economies using sound money principles to create sustainable healthy economies over long periods of time. The problem arises when

governments using gold standards, or other currencies backed by a commodity, find a *temporary need* to begin to debase their currency - the act of making pure gold coins into 50 percent gold and 50 percent copper, for example. MMT proponents point to these cases and say, "Hard money standards will eventually just turn into debased currencies or even pure fiat currencies, so why even try that?" And they would be right in that regard. That is why BTC, the world's first programmatic money with a fixed supply is so vitally important. This comes back to the decentralized nature of Bitcoin. It really doesn't matter if a government finds a *temporary need* to inflate their currency supply, because Bitcoin cannot be altered and therefore it is the first money standard in history that can be relied upon to not be debased. This is an absolutely astounding fact that 99.99 percent of the world doesn't get yet, and it points to the certainty that Bitcoin will be *the* monetary standard of the future.

CBDC's (Central Bank Digital Currencies) and the Dark Side of Smart Contracts

"CBDC's are surveillance disguised as money."

- Jeff Booth,
Author, The Price of Tomorrow
**Quote from his keynote speech at the*
Restart Vienna Financial Summit

Smart Contracts are a truly special innovation that deserves respect and even their own book. But, aside from what was discussed in the dApps section, we will discuss them alongside CBDC's here as well. Since much of this book looks at blockchain technology through a macroeconomic lens, we will discuss these two topics together. Where Bitcoin and smart contracts represent digital liberty, a level financial playing field, and new frontiers, CBDC's represent digital dictatorship and a new spin on the old guard.

CBDC's utilize much of the technology that has been innovated in the private-sector and open-source cryptocurrency industry (blockchain and stablecoins to name a few) but they do away with some of the fundamental tenets of Bitcoin such as censorship resistance and decentralization. CBDC's don't seem to attempt to hide this fact since the word "central" is right in their name. Governments will gravitate toward them for genuine reasons as well, considering that they would essentially do away with the black market industry of counterfeit currency overnight. CBDC's may prove to foster greater commerce both digitally and in person, but it's quite easy for one to imagine the various baggage that comes with them. We will briefly touch on a few of them here.

One of the interesting innovations of Bitcoin and its descendant Ethereum is that money or value can now be programmable. This means that money can do more than just go from point A to point B. Although we are discussing Smart Contracts here alongside CBDC's, which I have a very negative sentiment toward, Smart Contracts predate CBDC's and on their own, are a monumental technological innovation that will be an amazing tool for humanity. A smart contract is just a piece of code that executes a transfer of funds or other functions when certain conditions are met.

For example, a parent could choose to reward their child for a good grade with a smart contract. If the child gets a B, they get \$10. If they get an A, they get \$20. When the child's grades are posted on the school's website, that data is fed directly into the smart contract and the correct amount of money is transferred into the child's wallet.

Another simple example could be applying this technology to an existing industry - say, escrow services. If you have ever bought a house, then you are familiar with what escrow is. When a house seller and a house buyer decide to work together to execute a transaction they typically do not know one another and therefore cannot trust each other, especially with such large sums of money. So how can the house seller be confident that they can spend their time packing up their things and get ready to make an offer on their own new house when they do not know if their house buyer is really a trustworthy person? The house buyer puts their funds into a third-party escrow account. That third party provides security and trust for the entire transaction. While this practice has

worked quite well for ages, smart contracts enable the services of a very costly escrow company to be done by a few lines of code in a completely trustless and fair way.

A practical shortcoming of smart contracts in their current form is that they are written in programming languages. This is for obvious reasons. But, in a real-world setting it's easy to see how this can hinder their mainstream adoption. Currently, legal contracts are written in plain language and are relatively easy to understand. The more nefarious side of legal contracts occurs when skilled lawyers write complicated legalese into contracts to confuse a counterparty and thereby take advantage of them. Imagine the power that an unscrupulous programmer has in writing a smart contract. While this code is open-source and auditable, the everyday user would be incapable of auditing their contract effectively or in a timely manner. I believe that plain language smart contract languages will need to be developed before we see widespread adoption of smart contracts used in home escrows or business contracts. Even with this limitation, the use of smart contracts has exploded in many different sectors within crypto which is laying the foundation for wider use.

In spite of this technical issue, smart contracts are a great and novel concept. Thinking about potential applications of this technology for even a few minutes can cause one to see the tremendous potential of its utility. But, as with all tools, this tool can be used in ways that citizens of a country may not like. Citizens may like the fact that their government can more easily and efficiently distribute stimulus checks during a crisis, but if that stimulus check is programmable, then it could potentially come with restrictions. In times of economic depression, governments want individuals to increase their spending habits. In order to do this, they may stipulate that funds must be spent within a given period of time or they will be withdrawn.

On the other side of the economic crisis spectrum, how could a government use programmable money in a high inflation or hyperinflationary crisis - similar to the one that I and many macro economists predict is coming? Since inflation is caused by high money velocity - meaning that people try to spend their money as quickly as they can because it's losing value so quickly - central banks could freeze accounts or limit the rate at which individuals spend. Central banks could

also identify certain items that may be purchased while others may not be - stimulating certain economic sectors that are deemed more important. Being able to curb inflation would be a powerful tool for the Federal Reserve and would benefit society in that regard. But it could come at the cost of financial freedom.

“If you don’t have freedom to transact, you don’t have freedom.”

- Anthony Pompliano,
The Best Business Show

Another interesting benefit of CBDC's and programmable money is that economists will be able to track economic data better than ever. Most people would be surprised that economics is largely considered a *theoretical* field rather than a *scientific* field. Economists build models based upon theory and some real world data. But economic data has so many variables that it's quite difficult to track and understand because so much of the system is very opaque. For example, how do we really know what the impact of a tariff is on foreign car sales? We might see foreign car sales go down, but that tariff is really only one of thousands of variables that could affect these metrics, like weather, gas prices, political climate, unemployment, etc., that can change at any time.

One of the most important economic metrics for nations is their Gross Domestic Product (GDP). This is a measure of their total economic activity within a year. This information is aggregated through tax reporting and, surprisingly, surveys. It is evident that this is an inefficient means of getting an accurate number. CBDC's offer countries the ability to get precise GDP data. With highly trackable currency, for the first time ever, economists would be able to get a much clearer picture of how economies work and what the effects of monetary and public policies are.

In September of 2021, US President Joe Biden nominated Saule Omarova as the Comptroller of the Currency. Upon her nomination, she put forward two rather drastic proposals:

1.) All citizens would be required to have a Federal Reserve bank account, essentially changing the face of commercial banking as we know it and

2.) Social credit scores. If you are unfamiliar with social credit scores, I highly suggest that you take a 6 minute break from reading this book and go to YouTube. Type in *China's "Social Credit System" Has Caused More Than Just Public Shaming (HBO)*. This is an eye-opening documentary by Vice News from 2018.

The implications of these two proposals taken together are particularly troubling. Banks are already flawed in many ways (we will get into this more later on), but not having a free market option to choose your bank, paired with a social credit score based upon compliance with government regulations, has tremendous implications with regard to individual liberty. This in and of itself should be a trumpet blast alert to everyone on planet Earth to buy Bitcoin and become their own bank. Especially looking at these proposals through the lens of a post 2020 world, one can quickly imagine how governments could use coercive monetary measures via programmable money and smart contracts tied to one's social credit score to elicit compliance from their population.

You might think that vaccines are such a great and wonderful invention that they should be mandated, especially during a pandemic. And you may even be comfortable with a government decreasing someone's social credit score for not complying with a vaccine mandate, even if it meant their bank account was frozen until they inevitably complied. One might even argue that it's for the "greater good". But now imagine the other political party comes to power - one with which you do not agree. Maybe you believe that an individual should be able to transition their gender as a fundamental human right. But a new administration could use the power of social credit scores and CBDC's to circumvent the law and freeze the accounts of anyone that participates in a gender reassignment surgery.

Historically, rights are stripped and power is seized by governments in the name of a "good cause". Think tanks like the World Economic Forum have already put forth literature suggesting that CBDC

wallets should come with restrictions and limits for poorer citizens in the name of limiting their risk. The premise is that if a wallet could be hacked, then a poorer person would be financially devastated. So, limiting how much these poor individuals can store in a wallet and determining maximum transaction sizes as well as the frequency of transactions is being discussed amongst the economic elite. It's an oppression of low expectation. The thinking goes: because these individuals are poor, they must therefore be financially unsophisticated, and we must put more "protections" on their wallets to help them. While this might seem like one of Big Brother's more altruistic moves, it impedes poorer individuals from being able to advance and therefore keeps them reliant on a public entitlement system which often perpetuates poverty rather than individual economic development.

I do think there is a scenario where the CBDC's of some governments may not be instruments of authoritarianism. Because of the co-existence of free market competitors like Bitcoin, governments that have some sense of balance and liberty will be forced to exercise some restraint with the capabilities of their digital currencies or risk a mass exodus into a freer option. Whether governments create a digital currency for the purpose of surveillance and the restriction of financial liberty, or they develop a more liberty-minded CBDC, the very creation of a CBDC will be one of the biggest catalysts for the value appreciation of bitcoin.

One thing to note is that private companies essentially have an exemption to violating free speech laws. For example, Facebook is a platform that is not required by law to allow free speech. Facebook can censor anything they choose. As you will see later in this book, if you didn't know it already, the Federal Reserve is not a government agency. It is a private entity. Does this mean that the Fed can *lawfully* censor free speech via monetary sanctions of American citizens? This is an important point to consider with CBDC's going forward.

If I had to guess, I would assume that governments will take the more restrictive path with this novel power. The ability to have full control of a citizenry's finances is a powerful political tool that could be wielded at the expense of individual sovereignty and personal liberty. This most certainly crosses the line in a free society. One could even

make a strong argument that it fundamentally changes a Constitutional Republic overnight. The good news is that we have a tool that protects liberty, and its name is Bitcoin.

Hard Fork vs Soft Fork

When you are around the cryptocurrency or computing programming space for long enough, you will inevitably hear about forks. When it comes to open-source distributed computing (software that is open to everyone and run by multiple people), to make improvements, there must be agreement amongst those participating in the network. This is part of the democratic nature of blockchain.

When an upgrade to the protocol is proposed (in Bitcoin we call these BIP's - Bitcoin Improvement Proposals), miners can signal to the rest of the network whether or not they are in favor of the proposal. If a majority of miners are in favor of the upgrade, then there will be a fork, or a new branch to the software protocol and the old branch is dismissed by that community. It's like in *Back to the Future*. When Marty and Doc alter the past, a new future timeline emerges.

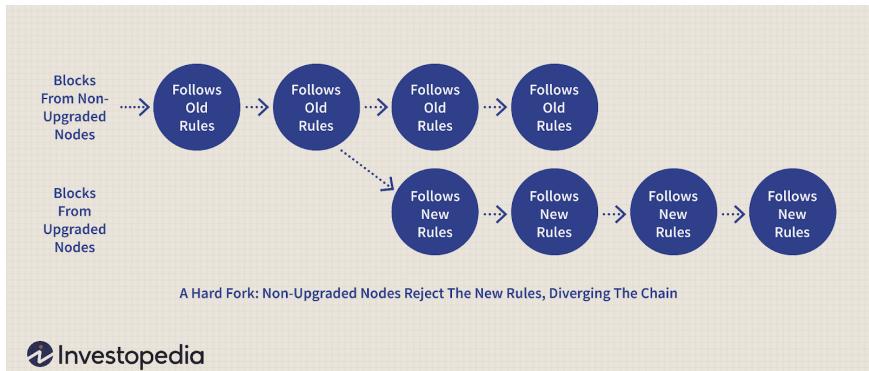
Now, it is possible for some miners to continue to run the old protocol and continue that chain if they so choose. This is also part of the democratic and free market nature of Bitcoin. When this happens, this is known as a hard fork. A **hard fork** is when new software is adopted, and the old software is no longer compatible. In the history of Bitcoin there have been some contentious hard forks in the Bitcoin community, and because these differences could not be resolved, multiple chains emerged. In 2017 there was a disagreement over a BIP that would change the size of the blocks in the blockchain. Because miners did not come to a consensus and the two communities of developers wanted to continue with their version of the chain, a new blockchain called Bitcoin Cash emerged to run separately from Bitcoin (or as the Bitcoin Cash community call it, "Bitcoin Core"). Shortly thereafter, another hard fork happened, and the Bitcoin Cash community split into yet another chain called Bitcoin Satoshi Vision (Bitcoin SV).

A **soft fork** is more common than a hard fork because the Bitcoin developer community is not intentionally seeking to fracture the

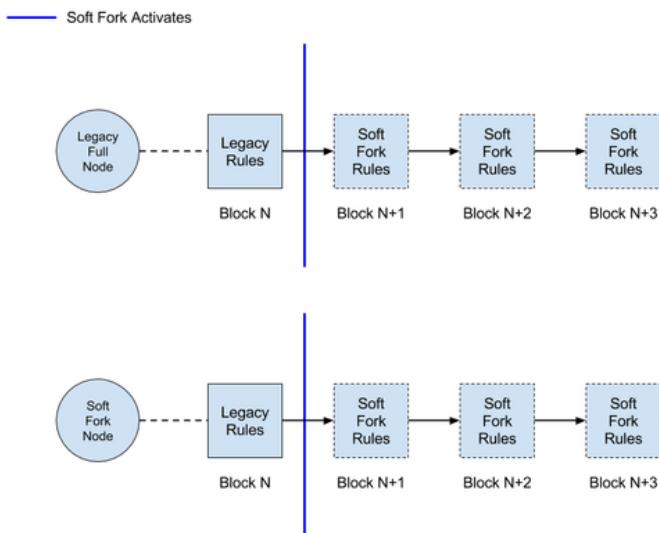
community, so it is a best practice to move forward with BIP's that are desired by the majority of the network. Soft forks are also less drastic changes to the protocol so in these cases, the new software is compatible with the old software. So, if some miners and nodes choose not to run the new software, they can still participate in the network. Soft forks are typically “gentler” improvements to the protocol.

A simple way to think about hard and soft forks with regard to existing technologies that most people are familiar with is to think about apps on our smartphones. We've all been asked to update our phone's operating system from time to time. Think of a soft fork like this: my wife, Alyssa, NEVER updates her phone's operating system software because she likes her phone the way it is. And most of her apps will still run just fine on her phone because their newer versions are backward compatible with her old software. She gets to stick with the older version of her phone's software the way she likes it and yet she still gets to use her favorite apps, even the newest version of it.

Using that same example, let's apply this to hard forks. While most of Alyssa's favorite apps are backward compatible with her phone's older operating system, some apps are not. For apps like Facebook to function properly or, in some cases, at all, you would be required to update your phone's *operating* system. This is akin to a hard fork because she has the freedom to not upgrade the software, but then she will no longer be able to participate in the Facebook network through her phone.



 Investopedia



HODL

In a society where memes and euphemisms are prevalent, it seems fitting that a novel technology created during this generation has a few of them itself. I am a millennial, so I have had a front row seat to the transition into the smartphone and meme generation and its characterization can most accurately be expressed as *informal*. I once did a business deal with hundreds of thousands of dollars at stake with a man over text message and upon me making my final offer, he confirmed that the deal was agreeable by sending nothing but a thumbs up emoji.

So, I suppose it is not entirely out of place in this generation to see mainstream financial television shows commonly throwing around callow-sounding terms like *HODL*. If you have watched those shows or heard your friend discussing crypto, then you have probably heard *HODL* used in its proper context - to keep holding BTC no matter what. If the price goes up, *HODL*. If the price goes down, *HODL*. The term has, in recent years, been given an acronistic meaning: *Hold on for dear life*.

While this attitude of holding on for dear life is most certainly fitting regarding BTC's volatility in terms of its US Dollar value, this is not actually where the term comes from. While Bitcoin is a world-changing technology that I believe will bring financial access equality to the entire world and lift millions of people out of destitute poverty (the effects a level playing field and financial innovation will have), the term *HODL*, as with many other things in *crypto* culture, has a belligerent beginning. The term dates back to 2013 with a post in the BitcoinTalk forum. That year the price of BTC surged to a high of over \$1,100 in December 2013 from just \$15 in January 2013 . On December 18th, in only 24 hours, the price of BTC fell almost 40 percent, to \$438 from \$716. Forum participants were in a full blown panic and discussions revolved around whether to sell or not. And that's when history was made:

At 10 a.m., GameKyuubi posted a rant with the title, "I AM HODLING," a drunk, semi-coherent, typo-filled explanation ensued. "I type d that tytitle twice because I knew it was wrong the first time. Still wrong. w/e, WHY AM I HOLDING? I'LL TELL YOU WHY," he

continued. "It's because I'm a bad trader and I KNOW I'M A BAD TRADER. Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a millino bucks sure no problem bro."

It may not be worthy of a Pulitzer Prize Award, but it hoisted a new term upon the world nonetheless.

Web 3.0 and The Metaverse

The internet has a very interesting and rich history, but we won't dig into that history here. Instead, we'll just scratch the surface as it pertains to the iterations of the internet known as 1.0 and 2.0. Internet systems existed in some capacity for decades before the advent of the world wide web, but Web 1.0 is acknowledged as starting in 1989. Also known as the "Semantic Web", it was revolutionary at the time because text-based information could be transferred around the world at the speed of light via email and web pages. Another name for Web 1.0 was the "read only" web. It was an amazing technology to facilitate chat rooms, online bulletins and forums, and to make blog posts. Although this was a huge innovation, by today's standards it was quite limited.

Web 2.0 is marked by more sophisticated ideations of Web 1.0. Mobile computing, cloud computing, video streaming and conferencing, online video games, and other more robust services define Web 2.0. Online commerce blossomed through Web 2.0 in terms of both payment platforms and increasingly efficient logistics. If Web 1.0 was the internet of information and Web 2.0 was the internet of content, then Web 3.0 could be described as the internet of value.

I believe that at some point we will stop referring to our industry as blockchain because it will be rolled up into Web 3.0 along with artificial intelligence, virtual or augmented reality, and the metaverse. At this stage it is somewhat abstract to envision how commerce will take place in Web 3.0 because we are really only at the very beginning stages of this phase. There will be an evolutionary process that happens by which commerce in the Metaverse will seamlessly interact with commerce in the real world. I believe people will have jobs entirely in

the metaverse where they will provide real value to other people - something that sounds silly by today's standards.

If talking about having a job in a virtual reality world sounds kooky or off-putting to you, do not let that be a distraction from this technology. Because Bitcoin and blockchain will have tremendous real-world value in addition to their value in these new artificial environments. Just keep in mind that people during Web 1.0 would have had a difficult time foreseeing teens being glued to their phones watching thirty second TikTok videos for hours on end or being able to have a personal butler (DoorDash) bring you food at any time of the day or night. So, it's helpful to have an open mind when it comes to learning about these things.

Chapter Three: *The 8 Qualities of Sound Money - and the New, Secret 9th Quality*

“Corrupt money leads to a corrupt society.”

- Larry Lepard,
*Founder of Equity
Management Associates*

Bitcoiners share many of the ideals of Goldbugs - those that are strong proponents of gold as money and a store of value. Often, these people (Bitcoiners and Goldbugs are one and the same), while some young Bitcoin enthusiasts think of gold as antiquated and irrelevant in a digital society, they must nonetheless recognize that gold has carried the banner for sound money for thousands of years. In fact, even the term “sound money” comes from an authenticating practice whereby a merchant would drop a gold coin and listen for its sound. This would indicate to a keen ear whether this coin was pure gold or if it had been debased with a cheaper metal inside.

Throughout history various items and commodities have functioned as money. Some worked adequately and some worked rather poorly, but humankind has been in a constant state of monetary evolution because no money in history has been perfect. Short of having a *perfect*

money, civilization has had *sound* money. Sound money is simply money that has some of the nine distinct qualities that make it reliable for such an important function. Of the nine qualities, the three most important are: store of value, limited supply, and acceptability.

Before we proceed, it is important to distinguish between currency and money. Money is what has some or all of the following eight characteristics. Something is considered at least semi-sound money if it has at least two of the eight qualities - the more of these attributes it has, the more reliable it is as money. Money is typically some sort of commodity like gold. Money can exist as money independent from a government declaring its value. Currency comes in two forms: commodity-backed and fiat. Commodity-backed currency would be a system where banks hold, for example, customer's gold, and in return are given certificates to be able to redeem their gold. Kind of like a claim ticket at the dry cleaner.

These paper certificates (currency) could be traded in commerce because they were reliable stores of value since whomever held the certificate could go and claim that gold from the bank. The phrase "it's as good as gold" comes from this system - when otherwise worthless pieces of paper could actually have tremendous value because they represented a claim to gold.

On the other end of the currency spectrum is fiat currency. As discussed earlier, fiat currency is not backed by anything other than a government decree that says it's valuable. In the case of the US dollar, it is backed by "the full faith and credit of the United States government." That might mean a lot to some people but those that have studied fiat systems of the past will recognize that they have a 100 percent failure rate.

Because colloquial use of the terms money and currency are interchangeable, I use them interchangeably in this book for the sake of readability. You don't need to get too caught up on the nuances between currency and money, but it is enlightening to understand the difference. Currency is not bad. And while the US dollar will get bashed considerably throughout this book, it's worth noting that it is currently the strongest form of currency in the world. It's just helpful to understand that there's a distinction between currency and money.

Before we take a dive into the qualities of money, it's important to ask the question, "Why is sound money even important?" For one, loose money policies are one of the enabling factors for unnecessary wars. If a country is invaded, a king could quickly raise tax money to fight a defensive war because the people will unanimously agree that their homeland should be defended against a foreign invasion. Citizens will gladly pay to protect their homeland. On the other hand, in the case of an offensive war where the benefits are less clear or important to the general population, it would be more difficult to raise taxes to fund the war. If the king is restricted to only raising funds when the population is in agreement, then many of history's "wars of vanity" would not have been fought. Things like imperialism would have existed in a far less common form.

Unfortunately, leaders have historically turned to loose money policies in order to push their agendas for war. Loose money policies enable leaders to do this because they fund their war efforts often without even a law being passed. They simply increase the money supply, and the population is none the wiser. This practice goes all the way back to the Greeks in 431 B.C. when Athens debased its currency to fund their war against Sparta in the Peloponnesian War⁽²²⁾.

It's likely not a coincidence that the 20th century was the bloodiest period in history as the founding of The Federal Reserve in 1913 and the founding of the various central banks across Europe ensued through the late 19th and early 20th century. Central banks are organizations that exist for the purpose of loose money policy.

In addition to war, bad money policies lead to unemployment, poverty, starvation, vulnerability to disease, and lost generations to drugs and mental disease. Bad money concentrates power into the hands of only a few. Society is left to the whims of those few powerful individuals - something that historically has not been beneficial to the masses. For a sustainably vibrant society we need good sound money.

1. Durability

Sound money should be durable. It should be resistant to bad weather, natural disasters, destruction by an enemy, rust, corrosion, decomposition, and time.

I was born and raised in Riverside, California, where I still reside. Riverside is like most US cities. There are nice areas as well as areas that are less desirable to live in. Since Riverside is located between San Diego, Orange County and Los Angeles - three of southern California's wealthiest areas - if you hear of Riverside referenced in a movie or a TV show, it's usually with a tone that makes Riverside sound like a ghetto. Because of this, many people are surprised to hear of Riverside's wealthy history.

Many of the groves that once defined our town have been torn down and replaced with development, but our city was originally a bustling epicenter of the citrus industry. Going back to 1882, there were more than half a million citrus trees in California, almost half of those were in Riverside. The development of refrigerated railroad cars and innovative irrigation systems established Riverside as the wealthiest city in the United States per capita by 1895.

Oranges produced vast amounts of wealth for the citizens of Riverside and they made the city a destination for movie stars, US Presidents, and foreign diplomats to visit. While oranges gave Riversiders tremendous wealth, no farmer held onto his oranges for any longer than he had to. How could something so valuable be such a poor store of wealth? Because it was not durable. As a commodity, they only economically benefit farmers once they are sold. Oranges are great at producing wealth, but they are terrible at maintaining wealth.

In stark contrast, bitcoin has excellent durability. Bitcoin does not rust, dilute, wane, or otherwise diminish over any period of time. Gold is also a reliable form of money because of this quality. Compared to perishable commodities like oranges or paper currency, gold and bitcoin stand head and shoulders above. If you wanted to store your

wealth for the next five hundred years, your only options in terms of durability would be gold or bitcoin. Everything else could have potentially turned to dust by then.

2. Portability

Sound money should be portable. One must be able to easily render money to someone they wish to do business with. For longer distance commerce, portability is absolutely essential.

For more than five hundred years the Yapese people of Micronesia have used Rai stones as their form of money. Rai stones were, and in some small villages still are, used in important social transactions such as marriage dowries, inheritances, political deals, diplomacy, war, and even essential staples like food. Rai stones are massive, quarried rocks that weigh as much as eight thousand pounds. One might wonder why these were used as money. It's simple. Because they were perceived to have value since they were so difficult to produce and thus difficult to counterfeit or have a high supply.

While the ownership of a particular stone might change hands, the enormous stone itself was rarely moved due to its weight and risk of damage. Therefore, the physical location of a stone was often not significant: ownership was established by shared agreement - something as simple as an announcement made to the village to let everyone know that Bob no longer owns the stone. Instead Gary owns it now. This was a very open and transparent system - something lacking today in the vast majority of monetary systems around the world. Each massive stone had an oral history that included the names of previous owners. In one instance, a large Rai being transported by a small wooden boat sank to the sea floor. Even though it was never recovered, the village agreed that the Rai must still be there, so it continued to be transacted as any other stone.

The perceived value of a specific stone was based on not only its size and craftsmanship, but also its history. The value could depend, for instance, on whether it was brought by a famous sailor, or whether people died during its transport. While Rai stones had some qualities of sound money like durability, limited supply, acceptability among the villagers and other nearby villages, it was dreadfully lacking when it came to portability. In fact, they were used because they were so difficult to steal, but it made it impossible to use them for commerce beyond a close proximity.

As westerners, we tend to think of monetary systems much differently than the rest of the world does. While we might not agree with our system entirely, we can argue that it has worked relatively efficiently up to this point. Interestingly, when you look at money's relationship with portability in more hostile nations, you may begin to see some of the inherent value in Bitcoin. Bitcoin allows individuals in countries with poor rule of law, corrupt governments, and dangerous political climates to take their wealth anywhere in the world in the blink of an eye. Imagine attempting to do this with cash, gold, or a cow. Your cash is no good anywhere else and it would be difficult to carry if you have even a moderately substantial amount. Gold would be quite difficult to transport. Your cow would be cumbersome and expensive to transport, and not very covert. And all three are at risk of being confiscated at any point by the hostile government or opportunistic thieves.

Bitcoin fulfills the quality of portability better than any money (or currency for that matter) in history. In an instant, bitcoin can be zipped off to any corner of the world that has an internet connection. You might say, what about parts of the world that don't have an internet connection? Projects like Blocksteam have initiatives to provide Bitcoin network broadcasting via satellite. Their homepage reads,

"The Blockstream Satellite network broadcasts the Bitcoin blockchain around the world 24/7 for free, protecting against network interruptions and providing areas without reliable internet connections with the opportunity to use Bitcoin."

Furthermore, because Bitcoin can be broadcast via satellite, this makes it the first hard money that is capable of being portable at an interplanetary level. No money can come close to competing with bitcoin on portability.

3. Divisibility

Sound money should be easily divided. Most sound monetary items are quite valuable, so it is important that they are divisible, with the capacity to be used for smaller transactions.

Cattle were among the earliest forms of money in ancient civilizations. Use of cattle in commerce dates back to 6,000 B.C. Aside from any religious value cows had as sacraments, they had tremendous value for their utility. Due to the perpetual milk supply, the ability to breed and produce offspring, as well as bulls' use in agriculture and as food, cattle were a very flexible commodity. This flexibility made them valuable to everyone - thus fulfilling the acceptability component of sound money.

Without universally desired commodities like cattle, barter was very difficult. Cattle acted as a bridge asset in commerce that made it possible to deal with virtually anyone in an economy. But cattle as money still had limitations. Imagine if you made rugs for a living and you wanted to buy sandals. If the lady that makes sandals does not need a rug, then you were going to have a hard time buying sandals. But if you could trade some rugs for a cow, then you were sure to have something that the sandal maker would want. Unfortunately, the problem you would run into is that your cow is worth one hundred pairs of sandals and you only need one pair. Because your cow is not easily divisible, it does not work well for these types of transactions and therefore, a cow is a very inefficient form of money.

Gold, historically the world's most reliable hard money, fails in the divisibility category as well. We love that gold is so precious and so valuable, but currently, a one-ounce gold coin (about the size of a silver dollar) is \$1,800. Even a tenth ounce gold coin (the size of a dime) is worth \$180. So, unless you wish to transact for only high value items, even gold, baby boomers' favorite hard money, is lacking.

Not only is bitcoin divisible, but it is also the most divisible money ever created. Earlier we discussed what a Satoshi or Sat is. It's the smallest amount of a whole bitcoin. In the same way that a penny is the smallest amount of a dollar, a sat is the smallest amount of a bitcoin. A bitcoin can be broken down into the eighth decimal place (0.00000001). Currently, one penny is the value of fifteen sats.

Why would anything need to be more divisible than the dollar? If we think only through our current lens, we may not be able to envision a reason. But when we put on our "innovation thinking cap" and think in terms of new paradigms, we can dream up all sorts of interesting uses for very small amounts of value, like in streaming payments. Currently, because of limitations on our money transfer systems, merchant costs where transactions under a certain amount are not cost efficient for businesses, it makes more sense to charge monthly membership fees for things like Netflix. But what if you could have the option to stream payments in incredibly small amounts and pay only for what you used rather than a monthly subscription fee?

What if, instead of having Facebook sell your data so that advertisers can target ads to you, you could own your own data and every time you chose to view an ad, you received a payment instead of Facebook? Highly divisible money will open up economies of scale and economic frontiers that we cannot even currently imagine.

4. Fungibility

Sound money should be fungible. This means that one unit should be worth exactly the same as another unit.

Fungibility is an essential component of both money and currency. In regard to currency, a one-dollar bill holds the same value as another one-dollar bill. If you are receiving change, you don't care which particular one-dollar bill you get because all dollar bills are worth the same. If individuals could not trust in the fungibility of their money or currency, the financial system would be very inefficient. Imagine if someone wrote a hateful or racist message on a \$20 bill and you received that bill in a transaction. You might think twice about accepting that bill. The bill says it is worth \$20, but you might refuse to accept that specific bill and would instead request a different one - that bill with the slur on it is no longer fungible.

This is one of the reasons why it is a crime to deface federal bank notes. According to the Bureau of Engraving and Printing under the U.S Department of the Treasury:

"Defacement of currency is a violation of Title 18, Section 333 of the United States Code. Under this provision, currency defacement is generally defined as follows: Whoever mutilates, cuts, disfigures, perforates, unites or cements together, or does any other thing to any bank bill, draft, note, or other evidence of debt issued by any national banking association, Federal Reserve Bank, or Federal Reserve System, with intent to render such item(s) unfit to be reissued, shall be fined under this title or imprisoned not more than six months, or both."

It kind of sounds like they don't mess around on this. Items like Rai stones and cattle were not particularly good when it came to fungibility. Rai stones varied in value based on their size and their oral history. Two stones may even be the exact same size but if one had been owned previously by a chief and the other stone never had a famous owner then the first stone would be more valuable. The same is true of cattle. One bull and another bull could vary quite drastically in terms of their market value.

Bitcoin and its smaller units (sats), are absolutely fungible. There is no difference between one bitcoin and another. Bitcoin cannot be defaced like paper currency. It cannot be counterfeited. You cannot sit two bitcoin down next to one another, as you can with bulls, and find any physical or qualitative differences between them. We flesh out this discussion a bit further in the “Not So Common Questions” section toward the end of the book. But for all intents and purposes, bitcoin functions perfectly as a fungible asset.

5. Limited Supply

[scarcity]

Sound money should have a limited and predictable supply. Scarce assets are more valuable than abundant assets.

Have you ever sat back and considered why Monopoly money isn't valuable? It is printed in specific denominations, it's fungible, and it even has utility. In terms of the physical item itself, Monopoly money is no different than USD. If you are playing a serious game of Monopoly you will find that the game's currency actually does have value because you can buy property, pay taxes, and earn income with it.

If it is valuable in the game, then how come it does not have value outside of the game? Because inside a game set, there is a limited supply of currency - \$20,580 to be exact. When you start the game, you are given 7.25 percent of the total supply of currency. From there, the point of the game is to accrue as high a percentage as possible, preferably all.

Monopoly money works inside of the game because it has a limited supply and the rules around the money are clearly defined. If you were playing a game of Monopoly and your friend pulled out a printer and started printing out more currency, you would say that he's cheating. The game is no longer fair because there are no longer just rules regarding the currency supply. It may sound silly to even consider

Monopoly money as a real currency, but currencies existing throughout history have had looser rules regarding their supply than in the game. Looking at whether the in-game currency would be a viable real-world unit of account provides an interesting thought experiment.

All the forms of sound money throughout history have had the quality of limited supply or scarcity. Going back to the example of the Rai stones from earlier, as strange as this system seems, it worked because the stones were scarce since they were so difficult to produce and transport. They had no intrinsic value, but entire societies could base their economy around them because their limited supply made them dependable. Trust in a society's money is absolutely essential for a healthy economy. This trust can be undermined when central banks drastically increase the currency supply.

As the world's first programmatic money, bitcoin is the only asset (aside from a select few other cryptocurrencies) that has a perfectly limited supply. There will only ever be 21M coins. Even with other famously scarce assets like gold, we don't know exactly how much is in circulation, nor do we know how much there is buried in the earth waiting to be dug up. Even if someday we were able to quantify how much gold is on the planet, there's no telling how much there is throughout the galaxy. Elon Musk has famously stated that he wants to mine gold from asteroids.

While that is a bit of hyperbole, it points to the idea that there is likely a near unlimited supply of gold in the universe. Whether there ultimately is or not, gold's supply is not knowable in the very specific way that BTC's is. BTC is the most scarce or limited supply asset in history because it is programmed to be that way - kind of an unfair technologic advantage that BTC has over all other forms of money.

Furthermore, when a commodity like corn goes up in value, farmers are incentivized to produce more. In this example, the price will have a supply and demand equilibrium, essentially keeping the price from rising too high. Although this commodity is scarce in one moment, there is a financial incentive for it to no longer be scarce the next season. Bitcoin is a better form of money than anything, ever, because its rule on scarcity was written in 2008 and has not changed since, nor will it ever.

No matter how much BTC miners are incentivized to produce more than the predetermined amount, they are unable to do so.

Important note: as we will see in the chart at the end of this chapter which compares gold, bitcoin, and USD, USD actually fares pretty well and checks off more categories than gold. USD is not considered sound or hard money because it fares so poorly in this one category of scarcity. This category is kind of like the trump card of sound money. If you have all other categories but lack this one, then you cannot be considered hard or sound money. Was it hard to make? Then it's hard money.

An easy way to think of what *hardness* of money means is to assess how difficult it is to produce said money. Fiat currency is as easy to produce as a few swift strokes on a keyboard. Gold takes enormous resources and labor to mine. BTC requires massive amounts of computing power to produce - thus making both BTC and gold quite hard. But the simple fact that USD can be debased so easily, undermines its role as sound money.

Because it is so strong in other categories, it is efficient as a currency. In fact, it is one of the strongest currencies of all time because the US has imposed its economic policies around the world and put USD in a strategically important macro position. Regardless, history tells us that all fiat currencies have a lifespan. Some are just longer than others. The US *dollar* has already far surpassed the lifespan of the average fiat currency due to its strategic strength.

The fundamental difference between a currency and money in terms of their value to the beholder is one's time horizon. Currency is efficient for buying things right now. Money should be efficient for commerce as well as storing and preserving wealth. For something to be a qualified store of value, as we will discuss in the following section, it must be trusted to not be debased and that can only be achieved by ensuring it has a limited supply.

6. Store of Value

Sound money should be reliable to hold its value over time.

Sovereign currencies like USD or the Euro are highly sought after. In movies, when an entrepreneur is daydreaming about success, he's usually imagining piles of cash. This is understandable because within the economy, cash talks. Everyone wants it because it can be later used to buy them whatever else they want. It's a very effective medium of exchange. But, because it's so effective as a medium of exchange, we often misconstrue that as being a good store of value. Store of value means that something has the ability to retain its value over time. Wealthy individuals use stores of value to transfer their wealth from one generation to the next.

In our school systems we often aren't taught much about finance. If you are taught something, it would be a very basic form of saving cash. Preserving wealth doesn't even enter the consciousness of most people. We get a very simplistic idea that our expenses are a certain amount and therefore to be financially healthy we just need some multiple of those monthly expenses in savings. While having an emergency fund and access to some liquid capital is prudent for investors, the majority of the net worth of wealthy individuals is not in currency, it is in assets.

Why is this so? Because the wealthy understand something that most people don't grasp (or if they do grasp it, they do not act accordingly): currency is *intended* to lose value every year. We will get into this further in the "Inflation Formula" section but when something depreciates at a certain rate every year, there is a compounding effect that happens over multiple years and decades where a small rate of depreciation snowballs in its effect and begins to have exponential consequences. For example, the daily wage of a skilled carpenter in 1850 was \$1.50. In 2021, a skilled carpenter makes \$221 per day - a 147-fold increase (14,700%). The value in the service that a carpenter provided

back then is the same as a carpenter today. What changed was the value of the currency they were paid in. As you can see, an average inflation target of two percent can destroy wealth across generations if that wealth is stored in the currency.

Bitcoin has proven to be an excellent long term store of value throughout its thirteen-year history thus far. Over the last ten years, bitcoin has outpaced the appreciation of history's favorite store of value - gold. At a time when gold's value proposition as a hedge against inflation should be at its strongest due to a decade of quantitative easing (currency printing), gold has appreciated from \$1,574 to \$1,799 (up 14%, 1.4% annualized). The stock market has gone up in value at a historic pace during the last decade as we have come out of the 2008/2009 financial crisis. The S&P 500 (an index of the stock market) has gone from \$1,267 to \$2,983 (up 135%, 13.5% annualized). Putting the rest to shame, bitcoin appreciated by 178% per year (17,800% total) during that same period. While both stocks and bitcoin outpaced inflation, bitcoin has shown it is the reigning champion in store of value. No asset in history has had a faster appreciation. An asset with such a meteoric rise and scarce supply makes the perfect recipe for an immaculate store of value.

INFLATION

Silently Robbing You Of Purchasing Power Since 1913



DEFLATION

Protecting you from the Federal Reserve since 2009

This meme is from 2017. While it's a bit hyperbolic and its price predictions didn't exactly hit, it does a fair job at making the point of BTC's proposition as a store of value versus USD.

7. Acceptability

[medium of exchange]

Sound money should be widely accepted. If individuals do not want it, then it functions poorly in commerce.

Gold has functioned as money for over 5,000 years. It has stood the test of time - wars, recessions, depressions, plagues, and revolutions. An interesting fun fact about gold is that the exact same gold that existed in ancient Egypt still exists today. The gold from the idol calf that Israel worshiped thousands of years ago, still exists. Gold plunder from pirate ships in the Middle Ages, still exists. Gold has been accepted by every major civilization in history. The United States became the world's preeminent superpower through selling munitions to Europe during World War I and II in exchange for gold. After WW2, the US held 75 percent of the entire world's gold⁽⁴⁶⁾. This led to the US dollar becoming the world's reserve currency.

Gold has a strange relationship with value and commerce. Gold is highly valued around the world but is almost universally not accepted by merchants for commerce. Everybody wants gold, but nobody will take gold. Hmm, quite strange. On the other hand, USD is widely accepted for commerce around the world. In fact, USD is the most accepted currency worldwide. Even though it is the most ubiquitous currency, there are still many countries that do not accept it either for political or utility reasons. Even for countries that do accept it, the legacy infrastructure has not kept up with 21st century speed. Sending a wire is a very clunky process. And while USD might be accepted within a country, if there is not a Western Union or a MoneyGram close, you will have a difficult time getting dollars into your economy.

Over the past twenty years, tech companies have made some incredible leaps forward in the realm of financial technology (aka: fintech) in modernized economies. They have made sending and

receiving payments much easier. But this is still a very “siloed” industry. By siloes, we mean entities that do not communicate with one another. For example, have you ever had the frustration of wanting to pay someone via Zelle but they only have Cash App? Even if you wanted to send someone a payment from Venmo to their PayPal account (owned by the same company) you wouldn’t be able to because these are closed off systems. They don’t communicate with one another. So, while the US dollar’s utility has become much more flexible through these innovations, there are still some pretty big pain points and roadblocks.

This is yet another category where bitcoin wins. One might say, “I can’t use BTC to buy a cheeseburger at my favorite restaurant, nor can I buy a car from a dealership with it. What are you talking about? It can’t be used anywhere!” They would be right that these establishments may not directly accept BTC. But because of technological innovations built around Bitcoin, someone that holds BTC can spend it while the counterparty receives whichever form of payment they choose. This means if you want to send BTC, and someone else wants USD, there are apps that make this transfer possible.

Companies like BitPay and Strike have built second layer infrastructure around Bitcoin so that these currencies and assets can be swapped in real time. Because of this, BTC is not only accepted in many places where USD is accepted, but it is also becoming accepted anywhere that there is a trading pair between a currency and bitcoin. Does the merchant want to be paid in Euros? No problem. Do they want Swiss Francs? Go for it.

BTC is technically accepted in every major country around the world. Furthermore, Bitcoin does not require the cost and infrastructure most businesses must go through to accept credit card payments. Anyone with an internet connection can accept bitcoin. Anyone with an electronic device that can receive a satellite signal can receive bitcoin. While it might seem clunky today, teams of developers all over the world are working to make this process seamless. There has never been a more flexible and widely accepted form of payment, ever.

Check out the infographic on the following page to get a visual representation of how this process works.



Payment in BTC > Receiving USD

Customer Has



using Bitcoin Lightning Network

Merchant Wants



*Strike utilizes a decentralized 2nd layer solution called the Lightning Network.
BitPay is a centralized 2nd layer option to facilitate payments.

8. Unit of Account

Sound money should be reliable for accounting purposes.

Imagine a time three thousand years ago when a farmer was calculating his net worth in a place where there was no currency. If he had forty cattle, he could mark that number down on some papyrus somewhere for his bookkeeping. That accounts for the quantity, but how would he account for the quality of his assets? How much is the farmer actually worth?

According to Curtis Craig, CPA, a partner at the accounting firm Genske Mulder that specializes in dairy accounting, a cow is typically two years old by the time she begins to milk. If twenty of those cattle are young and a year or more away from producing any real value, that is a significant difference from the farmer having forty fully grown cattle that he can already use productively. This drastically changes his net worth. Without a standard accounting unit, the farmer cannot accurately determine the value. A single cow is a poor accounting unit because cattle are not fungible.

A unit of account is a standard unit that helps individuals, businesses, and governments account for both quantity and quality and would be helpful for a cattle farmer, a factory, a small business, an individual, or any other entity to understand their true net worth and the value of their enterprise.

If there is an area where currency currently beats out sound money, it would be in its use as a unit of account. Many monetary purists choose to not include “unit of account” as a characteristic of sound money for this reason. But it is impossible to ignore the relevance of being able to properly account within the form of money or currency that one is using. What do you pay your taxes in? Dollars. Which accounting units do businesses keep their books in? Dollars. What units do businesses make their payroll in? Dollars. What are goods and services primarily priced in? Dollars. This has been a very efficient system for

accounting purposes. Businesses that provide widely varying goods and services, can all account in a common unit.

While bitcoin has not yet been adopted on the scale of the US dollar, the Bitcoin blockchain is the most audited and reliable accounting ledger in history. An enormous cost is incurred for a government to audit individuals or companies. Entire regulatory agencies like the Securities and Exchange Commission (SEC) require fantastically large budgets each year to oversee the practices of publicly traded companies.

Critically important institutions like The Federal Reserve have *never* been audited. I believe that because the Bitcoin blockchain is the most audited and transparent ledger ever, that governments, companies, and individuals will begin to adopt it to varying degrees. The incumbent system is totally opaque while Bitcoin is totally transparent. In the free market, which do you think people will gravitate towards?

The state of Ohio already allows its citizens to pay their taxes in bitcoin. Businesses like Overstock.com have accepted bitcoin as a form of payment since 2014. Companies like Coinbase and Strike have services that allow individuals to receive their paycheck or a portion of the paycheck in BTC. The country of El Salvador made history when it became the first sovereign nation to recognize BTC as an official currency.

I would be remiss to not mention that saying BTC can serve as a unit of account is the most highly contentious quality of BTC as sound money. A good friend of mine that is also a bitcoin-lover and a CPA would disagree that BTC serves as a unit of account. I do not fault him for having this opinion because his experience is such that he lives in accounting and, in his world, they use USD. I suppose this point will not only take scrutiny from him, but also from traditional thinkers.

It is a paradigm shift to think of accounting in terms of BTC - quite possibly much in the same way that people from the 1700s could not have imagined someday communicating to anyone around the world via “magic” frequencies that can transmit voice and video. That would have appeared more akin to black magic than science. Thinking of BTC as a unit of account for the Puritans of Accounting may similarly seem like practicing the dark arts rather than science.

We have only seen the first generation or two of adoption with BTC building the required foundation for it to be used as a widely recognized unit of account. Countries like El Salvador and The Central African Republic have shown us that there is true value for smaller countries to use BTC as currency rather than only the US dollar (they do not have their own sovereign currency), because the Bitcoin ledger is transparent while the USD ledger is totally opaque.

Since these small countries have been geopolitically influenced to be on the dollar standard, they are hurt by the Federal Reserve's lack of transparency. Imagine being a sovereign nation that is beholden to another country's monetary policies in which you have no say. If a country is not powerful enough to have their own sovereign currency, the next best thing is for them to have an open, fair, and transparent money system.

Small countries, adopting BTC as national currency, are paving the way for BTC to be used in traditional accounting as a proper unit of account. So, while USD is currently winning the battle, bitcoin will win the war.

9. The New and Secret 9th Quality: Digital

In a digital society, sound money should be digitally native.

You will not find this quality of money in any textbook. However, you might find it in the textbooks of the next generation. It is simply a logical conclusion about the present era that we find ourselves in - one that is defined by digital information, digital commerce, digital entertainment, digital education, and even strangely novel innovations like digital worlds. According to Jack Dorsey, the current CEO of financial technology company Block and the former CEO of Twitter, the internet will inevitably have a native currency. In his words,

“The internet is going to have a native currency, so let’s not wait for it to happen, let’s help it happen.”

For some, the advantage of digitally native money is obvious. For others, the efficiencies may not be so apparent. On October 26th, 2020, there was a \$1.15 billion transaction on the Bitcoin network - the fee was a mere \$3.58. That fee is obviously small for such a massive transaction, but to put that in perspective, to send \$1,000 via traditional payment rails (wire transfer, ACH, Western Union, etc) from the United States to the United Kingdom, it would cost \$25. In other words, a one million times *smaller* transaction would cost 6.9 times *more*. Nevermind the fact that Western Union would not wire a transaction as large as \$1 billion dollars. In fact, if you attempted to send over \$10,000, you would have to fill out additional paperwork to make sure you are Anti-Money Laundering (AML) compliant.

Credit card merchant fees for small businesses typically range from 2.5-3.5 percent. This means that when you swipe your credit card at a business, Visa/MC is charging that merchant as much as 3.5 percent of the purchase price. While this might not initially bother most consumers because they do not pity the business, they should realize that businesses are not dumb. They factor this cost into the price. So, when someone purchases a \$100 item, they are going to pay an additional \$3.50 - about the same as what it would cost to transfer \$1 billion dollars on the Bitcoin blockchain. Based upon the above example, a ten million times smaller transaction costs about the same as using bitcoin. Game over yet?

A logical question that could follow is, couldn’t Bitcoin miners just raise fee costs in the same way that Visa/MC do? On Bitcoin, fees can fluctuate due to usage but because miners are all competing against each other, there are market forces that keep fees in check. Visa and Mastercard have been sued over colluding to raise fees. Bitcoin’s decentralized nature prevents widespread collusion because there are millions of node operators that are largely unknown to one another.

The key difference in the fee structure of Bitcoin vs Visa/MC is that the fees actually aren’t dictated by the miners, the fees are bid by those sending a BTC payment. When you go to send a BTC payment,

you choose whatever fee you want. If there is high network traffic, you may want to incentivize miners to prioritize your payment by bidding a higher fee, but that is entirely optional. This concept of a fee bid structure flips the traditional model on its head and grants power back to those holding and transferring BTC. This is a feature that provides equilibrium of power in the Bitcoin ecosystem.

Let's go further on the example above. That \$1 billion BTC transaction settled with finality in ten minutes or less. According to Western Union's own website under "how long do international bank transfers take?" it says:

Depending on the bank, international bank transfers can take longer than you might expect. Once you've submitted your transfer request, the bank will follow its usual procedures. Each bank has its own cut-off time, which means if a request is not submitted before the cut-off, it won't be processed until the next business day. From there, most international bank transfer times are quoted as 1-5 business days. However, some factors may affect this timeframe.

Western Union's core business of international wire transfers is orders of magnitude slower and more expensive than Bitcoin. One has to imagine that banks and international money transfer companies had a chill run up their spines when they realized what Bitcoin truly is. The sheer fact that they operate using analog currency rather than Bitcoin's native digital currency puts them at a disadvantage that they will not be able to overcome. These companies have already been put out of business, they just don't know it yet.

Not only does digital money work better and more efficiently than analog currency, but governments - the makers of analog currency - are trending toward an entirely digital financial system themselves (Central Bank Digital Currencies, CBDCs). I believe in ten years physical currency will cease to exist, or at the most, it will be used only in a very limited capacity, or for nostalgic purposes. So, if private forms of money are all digital and government forms of currency are all digital, there's not much choice here. We will all inevitably adopt digital. If we are

going to do so, then it's of the utmost importance that we adopt a sound money.

In conclusion, you may have noticed that BTC wins, or will ultimately win, in all these categories. Why is that? Is it just by chance? No, this is one of the inherently valuable things about a digital form of money. You can start with first principles and then build around them. Gold already existed and out of all the commodities on Earth, it just coincidentally happened to have some of the same qualities as sound money. With BTC, it was the opposite. Sound money principles existed first, and then BTC was intentionally programmed to have those precise qualities. This is one of the unfair advantages that digital programmable money has over all other forms of money.

When assessing this chart, it's important to note that this only shows a yes/no for each category. It does not qualitatively rate each category. So, while USD checks off one more box than gold, categories such as limited supply and store of value carry much more weight in determining an asset as sound money.



Sound Money Checklist



	Bitcoin	Dollar	Gold
Durability	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Portability	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Divisibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fungibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Limited Supply	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Acceptability	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Store of Value	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Unit of Account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Digitally Native	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Chapter Four:

The Nine (ok, Ten) Tenets of Bitcoin

“New products and new methods compete with the old... not on equal terms but at a decisive advantage that may mean death to the latter.”

- Joseph Schumpeter,
Finance Minister of German-Austria, 1919

Up to this point we have discussed sound money and money’s historical relationship to economies. Now we will discuss the core tenets of Bitcoin. Before the evangelist can take to the streets and start spreading the good word, they need to understand the basic elements of their belief. An evangelist is left ineffective unless he or she is prepared. The following points are not only informative for one’s understanding of Bitcoin and blockchain, but they are helpful to fully reinforce one’s comprehension so that conversations with friends and family regarding fundamentals are informative rather than sounding like a pitch for some kind of get rich quick scheme.

1. Decentralized

The concept of decentralization is axiomatic. But, digging down into it a little bit further really helps illustrate what a wonderful tool

Bitcoin is. If fiat currency was a country, it would be a monarchy. If Bitcoin was a country, it would be a democracy.

Why does a \$20 bill have value? About a year ago I asked this question to a close family member. This family member was in their sixties at the time. I only mention their age because they had the distinct experience of living in both the era of the US dollar being gold-backed as well as the era of the US dollar being fiat-backed (to say something is fiat-backed is quite tongue-in-cheek and could be accompanied by a “wink face” emoji, as a forewarning to the newly initiated). This individual’s response was that the dollar had value because it was backed by gold. With what I’m sure was an unnecessarily arrogant tone I said, “do you know that this year is the 50-year anniversary of President Nixon taking the US dollar off the gold standard?”

My glib remark inhibited the conversation from going any further. I’ve brought up the question of why the dollar has value countless times in other conversations with business people, college professors, doctors, investors, and others, and the majority are unable to articulate a very specific, let alone accurate answer. The reason is probably because the US dollar, the world’s most widely used currency, only has value because the government says it does. That’s a very unsatisfying answer. It’s not a very sophisticated answer. And it just goes to show that even some of the smartest and most educated individuals do not understand where the value comes from for the one thing they spend one third of their life trying to get.

Going back to our original illustration of fiat being a monarchy and Bitcoin being a democracy: the king of the monarchy would be the Federal Reserve and the banking system. The Federal Reserve, aka “The Fed”, has the power to implement policies that affect the value and the supply of the dollar. What the king says, goes. If fiat currency is a monarchy under the Fed, and bitcoin is a democracy, what does this say about bitcoin? It’s pretty simple. Instead of a central individual authority, bitcoin has a set of rules similar to the American Constitution and a body of voters (miners and nodes).

This set of rules says that anyone who wants to, can join the network and participate as long as they abide by the rules. These rules are not reinforced by the honor system. They are reinforced by computer

code that disallows anyone from playing against the rules or gaming the system. But, with a pure majority vote of 51 percent, the rules can be changed and upgraded. Individuals are incentivized to act in the best interest of the network because by doing so, the value of the network, and their holdings, increases. Value and power are distributed to the participants rather than hoarded at the top of a pyramid.

Until October 31st, 2008, when Satoshi Nakamoto published the Bitcoin Whitepaper, the only type of financial systems that existed were centralized. Whether we are talking about large-scale nationwide central bank systems that dictate a country's monetary policy, or smaller bank and money transfer institutions that handle the accounts of individuals and businesses, it is all controlled in a top-down fashion.

The Bitcoin network is the world's first decentralized monetary system that has no president, no board, no employees, and no central authority. Satoshi publicly published the open-source code so that anyone that wished to, could participate in it. The Bitcoin network does not discriminate or dictate because it has no ability to. Its very nature is that it must allow any participant to enter - this actually lends itself to the security of the protocol, which we will get into later. It's a pretty interesting thing to contemplate. Human civilization has existed for thousands of years, but the first open and fair financial system ever, happened to be created within our lifetime. This is truly something special and we are privileged to be early adopters.

2. Peer to peer money

The heading of the Bitcoin Whitepaper reads "Bitcoin: A Peer-to-Peer Electronic Cash System". When Satoshi released the Bitcoin whitepaper on October 31st, 2008, it was the first ever workable peer-to-peer electronic payments system in history. It took some time before even the internet nerds took Bitcoin seriously, though, and early online forum responses to the whitepaper were generally pretty pessimistic. Projects dating back to at least the 1980s had attempted to create such a system, but failed, and most knowledgeable individuals in the field of computer science and cryptography were rightfully skeptical. But they were wrong.

Many people think we already have peer to peer money. They say, “When I Venmo \$10 to my friend for lunch, isn’t that peer to peer?” And while that thinking seems logical, it is not accurate. Our current financial system (Venmo, Visa, Mastercard, Western Union, ACH, etc.) uses payment rails to route payments from one person or entity to another. But traditional payments are much different than peer to peer payments, because in the current system, every time we send funds, we are essentially asking permission to do so. One might say, “I don’t ask permission to spend my money.” Try buying something your bank doesn’t approve of. Or try to buy something from a country that is being economically sanctioned. This might not be a day-to-day struggle for you, but it does illustrate the point that in traditional payment systems, we need permission to spend our funds.

Regardless, in the context of world history, this is a very efficient system. Currency (actually, just messages like a bank IOU) can be sent in seconds to many places all around the world! The ancient Egyptians, the Romans, not even 1st world nations of the early 20th Century had this luxury. While the payment rails associated with the current financial system have benefited society through greater commerce over the last 50 years, there is also a tremendous amount of inefficiency and counterparty risk in the context of a post 2020 world.

The incumbent payment rails of Visa, Mastercard, ACH or even newer entrants like PayPal, Cash App or Venmo, have not been able to provide a peer to peer monetary system. Why not? Because it’s not in their best interest to do so. Their businesses are predicated on being a middleman. Let’s imagine that you (Person A) want to send a Visa payment to your friend (Person B). You may think that means there are only two parties involved in this payment. That isn’t true. There are typically five or more parties involved in that transaction.

Person A wants to send \$10 to Person B.

*Person A initiates payment.

*Person A’s bank (Wells Fargo) verifies account balance and forwards payment approval to the payment rail (Visa).

*Visa transmits payment to Person B’s bank (Bank of America).

Transaction pends until the standard 24/48-hour window has passed.

*Person B can spend said \$10.

By comparison, the “middleman” in a Bitcoin transaction is simply a non-sentient algorithm that takes inputs and makes outputs. This means there is a network of computers that runs a program that simply says when Person A puts in \$10, out comes \$10 to Person B. There is no person or entity standing between Person A and Person B. This means there is no one to decline the transaction. There is no potential for disagreement between rival banking institutions regarding how the transfer should be handled.

This means there is no discrimination of either individuals involved in the transaction or what kind of good or service is being bought and sold. Lastly, this means that a digital transaction isn’t being broadcast with great detail to your financial institutions, including information regarding what you purchased, where you purchased it, when you purchased it and from whom. Many do not realize substantial detail about each transaction they make is kept, and often sold by financial institutions.

In the history of computer programming up until 2009 when Satoshi created Blockchain, there was no way for a digital transfer of value without someone overseeing it. Digital systems are particularly good at being *centralized* because they provide greater efficiency for institutions to exert control and monitor transactions. The Bitcoin whitepaper marked the first time in history that a digital system could truly achieve *decentralized* peer to peer money transfer.

SENDING FIAT VS BITCOIN

FIAT CURRENCY



Intermediaries bring you
high fees, restriction, slowness, closures

BITCOIN



Bitcoin network is
open, peer-to-peer, secure, instant, minimal fees



(49)

Chart courtesy of Crypto Explorer's Facebook Page

3. Censorship Resistant

Quite possibly the most important attribute of decentralized blockchains is censorship resistance. The implications are massive. Even the greatest democracies and fairest societies throughout the ages have histories of trampling on the rights of its citizens. The flaw with any system of government is that people can always break the rules. In the United States our 1st Amendment guarantees the freedoms of both speech and religion. Even being a nation of law and order, there are still plenty of court cases, even in recent history, where these rights have been violated. Blockchains take human corruption and error out of the system.

Some individuals will argue that censorship isn't that treacherous. But history shows that censorship is a prelude to authoritarianism. Censorship is a precursor to all sorts of violations of individuals and people groups. Throughout the post-2020 era where there are plenty of social and political tensions, I have consistently been objected to by well-meaning friends that say, "Do you really want to die on that hill?" My response is always the same. "No, I don't want to die on this hill. I want to defend this hill. By the time we get to the hill that gets you off the sidelines, you surely will die on that hill. Fight on the hill you can defend, not on the hill on which you will die."

With Bitcoin, censorship is a hill we can defend.

"Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same, or one day we will spend our sunset years telling our children and our children's children what it was once like in the United States where men were free."

- President Ronald Reagan

One of the great qualities of bitcoin being peer to peer money is that there is no central authority. This means there is no entity that can

block transactions. Another way of saying this is that Bitcoin is *permissionless*. All existing payment systems require the permission of one's financial institution, who is not just beholden to their own board of directors, but also government regulations and laws. Skeptics and lovers of Big Brother might find Bitcoin's censorship resistance problematic because they have heard stories of BTC being used to buy items on the dark web and they do not trust individuals with the power to make decisions over their own purchases. First of all, while it is true that BTC has been used for illicit activities, its use pales in comparison to the amount of US dollars used in these same activities.

If you tried to guilt someone into giving up their bank account because it was filled with US dollars, they would quickly give you what I think is an appropriate answer. They would tell you that money is a-moral. It is just a tool that is neither good nor bad. They would continue on by saying things like, you can use a hammer to build a home for a family or you can use it to assault someone. You can use it for good and you could use it for bad. So, because of that, they will refuse your guilt trip to give away their bank account, rendering this same argument against BTC moot.

I don't know if this is specifically true, but I heard it from a missionary one time and I think it's a cool analogy so I'll share it here. The two most purchased items on the black market are heroin (no surprise) and Bibles. Now, you might not find the Bible as valuable as I do, but this just goes to show that money can be used for the ultimate bad or the ultimate good. The problem comes in when governments or other authorities believe it is their duty to police the purchases of their citizens. Historically, this has been the catalyst for greater encroachments on human rights.

One of Bitcoin's incredible qualities is that it is censorship resistant. The most powerful person on the planet could tell you not to spend your BTC, but if you chose to anyway, they could not stop you. In recent years, firms like Chainalysis have created very sophisticated algorithms that do an ok job at tracking transactions across the Bitcoin blockchain. While more sophisticated Bitcoin users can obfuscate their transactions to remain private, and future innovations by the Bitcoin developers will surely make transactions more private for all users,

Chainalysis software currently has the potential to track some transactions. But there is a big difference between someone being able to *view* your transaction and being able to *stop* your transaction.

Chainalysis, other similar entities, and governments, all have the ability to *observe* transactions, but they have absolutely no ability to *stop* your transactions. Bitcoin as a technology is an incredibly powerful tool, especially for those that value individual liberty.

As I briefly mentioned earlier, in 2009, China began pilot testing *social credit scores* (SCS). Similar to a financial credit score, a SCS can get you access to work opportunities, loans and housing. But unlike a financial credit score, a good SCS can give you access to public transportation, social status, awards, other public services, and more. The converse is that a bad SCS can prohibit you from these things. If you did not do so earlier, please go to YouTube and search for “Vice - Chinese Social Credit”. They did an excellent and brief report on this subject. Social credit scores are based upon what is deemed good or bad social behavior. If you litter, five points are subtracted from you. If you clean up trash, you earn five points. Seems benign until you see social credit scores being downgraded by people publicly speaking out against the regime in power or voicing an otherwise unpopular opinion.

SCS’s have begun to creep into the post-2020 west. Canada has openly lauded the benefit they would bring. Prime Minister Trudeau even publicly expressed his admiration for what he called China’s “basic dictatorship”⁽⁵²⁾. SCS’s will empower governments to censor individuals by saying, “They weren’t good citizens anyway.” Or worse yet, they will potentially mis-label dissidents as racists and terrorists.

We live in a time where culture is very divided on issues of liberty and coercion. If you fall on the side of liberty, then bitcoin is an essential tool for you. For you, it is not a speculative asset or a luxury. It is necessary as a way to opt out of the prospect of coercive social systems. Bitcoin is a tool that can protect individuals’ medical, religious, and financial freedom. Ultimately, I believe that before social pressures effectively lobby socialist politicians to move against Bitcoin in any meaningful way, there will be enough adoption among institutional investors and the population as a whole that it will be difficult for the antagonists to gain much momentum. Nevertheless, some

macroeconomists believe in a much gloomier picture. This gloomy picture isn't one of Bitcoin. It's a gloomy outlook on further government overreach. Bitcoin the network, and BTC the digital asset, are the way to hedge oneself in such an event.

"There's such a big divide and a segregation happening among the population and even if bitcoin were to go to half (in price) it would be worth it just to have some (now) because if you get kicked out of the banking system, you might not be able to legally acquire bitcoin in the future."

- George Gammon,
Macro Economist

Whether it is blue skies ahead or a very dark and gloomy forecast, BTC is a form of insurance against many different outcomes by ensuring individuals have sovereignty over their own money and a powerful tool to opt out of centralized systems of control.

4. Fixed Supply (21M coins)

This is one of the simplest and most straight forward aspects of Bitcoin. Scarcity is programmed into the Bitcoin code. In fact, the advent of Bitcoin marked the first time in history that something digital could be made scarce. Prior to Bitcoin, anything digital could be replicated infinitely (more on that later). Satoshi Nakamoto created the Bitcoin code with an eventual supply cap of 21,000,000 coins. At inception there was no BTC in existence until the first block was mined where a block reward of fifty coins were minted. Since that first block on January 3rd, 2009, the supply of bitcoin has been steadily increasing at a predictable rate that diminishes over time and culminates with a total supply of 21,000,000 by the year 2140.

Imagine two scenarios. In one scenario your boss tells you to design a building. She gives you no instructions. It is up to you to

conceptualize what she wants. By chance, your building design may have some of the attributes she was looking for, but it is unlikely to be a perfect representation of what she wants. In the second scenario your boss asks you to design a building and gives specific instructions that it is to be a school for elementary age children and that she wants spacious classrooms and a playground with both a grass area and a blacktop. When you understand the qualities that need to be incorporated into the project, you can formulate your design around them and make your boss happy. If you don't have specific instructions, then the chances are your designs will be nowhere close to what your boss wants.

As we discussed earlier, one of the unfair advantages of BTC over all other previous forms of money is that it was able to start with first principles of what makes sound money and then program its code to suit those principles. In the same way that an engineer would design a better building if they had specifications, BTC was engineered to match all the qualities of money. Of the nine qualities of sound money, scarcity is among the three most important (the others being acceptability and store of value).

It is important to note that most cryptocurrency projects do not share this same characteristic with BTC. Coins like ETH (Ethereum) do not have a fixed supply. So, while they will share some properties with BTC, this fundamental economic component is missing.

5. Trustless

Trustless is a term widely used in the blockchain space, but it is not unique to it. Trustlessness (that's probably not even a real word) is a quality available in anything that is algorithmic, but it was given new applications when Satoshi Nakamoto invented Bitcoin. Trustless does not mean that the Bitcoin network cannot be trusted, and it does not mean the opposite of trust. In essence, trustless means the lack of a *need* for trust. That's kind of abstract, so let me try and explain it through a simple analogy.

Stop lights are algorithmic. When north and south bound traffic have green lights at a busy intersection, a program (aka an algorithm) turns west and east bound traffic lights red. If this algorithm failed, the

results would be catastrophic. But, let me ask you, when was the last time you drove through an intersection at 40 or 50 mph and panicked as though your life was in danger? Were you consciously placing your trust in that intersection's stoplight algorithm as though your life depended on it? No, because algorithms are trustless. It goes beyond trust, it's the removal of even the very need to trust. You just use it because it works every time.

That may be an overly simplistic way of thinking about the term trustless so let's dive a little bit more into the Bitcoin-specific application of the term. There's a common saying in the Bitcoin community, "Don't trust, verify." One of the beautiful features of the Bitcoin ledger is that each and every transaction is recorded for everyone to see. This doesn't mean that other people know what you have spent your BTC on though - your identity is encrypted. But the record of the transaction is on the blockchain permanently. Essentially, what it looks like to everyone else is that Person A sent X amount of BTC to Person B. So, if there is ever a discrepancy about whether something happened or not, it is quite easy to go to the Bitcoin Block Explorer (<https://www.blockchain.com/explorer>) and verify whether it happened or not.

"Don't trust, verify" also applies to the "constitution" or "rule book" of the Bitcoin network. If you want to know how the Bitcoin blockchain works, you can read the whitepaper written by Satoshi Nakamoto for yourself. It is only nine pages long and for your extended reading pleasure, I have included it in the Appendix. Lastly, "Don't trust, verify" also applies to the very code of the Bitcoin network. Bitcoin code was written in a common programming language called C++. Anyone can audit the entire code at any time to ensure that there are no bugs or back doors for bad actors.

6. Pseudonymous

This is a very quick and easy concept to understand. Bitcoin transactions are not anonymous because there is a little bit of on-chain data that identifies actors on the network. This isn't a personal identification in the sense that the network knows your name. But it does show a very rudimentary record of the participants on the network. The

term pseudonymous just means that you are using a false name. So instead of James Medina using his actual name on the blockchain, he would just use a public address. Rather than James Medina, the Bitcoin network would simply see User A. More specifically, James's public address would look something like this:

14qViLJfdGaP4EeHnDyJbEGQysnCpwk3gd

7. Fungible

We briefly covered fungibility earlier in the qualities of sound money section. I will cover it here in a more BTC-specific manner. Fungibility is a quality that is relevant to cryptocurrency because it is a quality that is relevant in traditional currency, due to its predictability. Fungible simply means that items are interchangeable. For example, if I told you that I was going to pay you \$1 for something, would you care which \$1 bill I gave you as long as it wasn't counterfeit? Probably not, because no matter which \$1 bill you received, you would be able to take that bill to any store and use it.

Fungibility, aside from just being a very fun word to say, is one of the chief selling points of Bitcoin. The Bitcoin ledger performs a full and transparent system wide audit of the entire blockchain every ten minutes. This ensures that one bitcoin always has the same value as another bitcoin. Counterfeit coins are an impossibility because all coins are accounted for 144 times per day. If a node on the network attempts to double-spend the same coin twice, hundreds of thousands of other nodes around the world will see it and that miner's block will be disregarded and excluded from the chain. It's the equivalent of trying to steal an old woman's purse inside a police station.

There is a nominal but relevant concern that all Bitcoin may not be fungible. If a particular Bitcoin was shown to have been used in an illegal transaction at some point in the past, some would argue that coin is less valuable in the same way that "conflict diamonds" are less valuable - because they have a shady past. I usually find this argument a bit hypocritical because those making it are strong proponents of the US dollar, which is used in far more illicit activity than any other instrument in human history. I mean, according to MarketWatch⁽¹⁾, 80 percent of

bills in circulation have trace amounts of cocaine on them. Probably nothing to see here...

8. Immutable

Much of Bitcoin's appeal comes from its immutable nature.

Immutable simply means unchangeable. You may have read lines earlier in this book such as, "The Bitcoin ledger cannot be changed". Maybe you wondered how it is possible it cannot be altered. The answer is quite simple. Because miners and node operators all over the world are auditing the entire ledger every ten minutes, if any errant change was made, millions of nodes all over the world would see the change and disregard it.

Immutability is a very important element when we are discussing a global monetary system. The record keeping for the world's money shouldn't be something that can be manipulated. Under our current central banking model, there is a singular group that controls the monetary system for the entire nation. Immutability is yet another element of Bitcoin that makes it novel. No ledger in history is immutable. JP Morgan Chase has full autonomy over their books, as does any other bank. While it would be highly illegal and unethical for them to adjust accounts at their will, it is not impossible. Bigger frauds have been perpetrated in the past. When a central authority has power over records, it thus has the power to change them.

A critical part of the plot in George Orwell's novel *1984* is that there is a government entity tasked with altering the recorded history in order to manipulate the population. This duty was performed by The Ministry of Truth. While the story is fiction, it points to the glaring fact that all we know of the past is what we are told. Whomever has the power to change the record books, the ledgers, and the traditions, has the power to control everything.

Bitcoin's decentralized nature makes changing the history of the ledger impossible. Once a block is added to the chain, it is set in stone and cannot be altered. Someone might ask, "Couldn't someone just hack the system and change it?". This is a good question, but the answer is no, because every node on the network (people that run nodes can be miners

or just individuals that have a full node wallet) keeps a record of the blocks and what is stored in them. This means that the hacker would have to simultaneously hack tens of thousands or even millions of devices to achieve this. And while movies might make this seem possible, I can assure you it is not.

This might beg the next question, “Couldn’t someone just submit a fake transaction to the network and game the system that way?” Also a good question. But again, the answer is no. Let’s envision a very basic decentralized network to make this point simple. Imagine a room with ten individuals sitting in a circle, each with a notepad to keep record of transactions. Each ten minutes a new set of transactions is batched together and each of the ten individuals writes down all the transactions on their notepads. Once they do, they show all the other people in the room their work to make sure they all have the same answers.

Now let’s say that an eleventh person sits down to record transactions. If he attempts to include a transaction that isn’t real, at the end of the next ten minutes when everyone shows each other their work, the other ten people will notice that he is wrong, and they will exclude his transaction from the official record. Items are only added to the official record when there is a consensus.

In the same way that these individuals could reach consensus by showing the entire room their work and verifying that they all have the same information, the Bitcoin nodes do the same thing. Once something has reached consensus, it is added to the chain... forever. While we must have trust that the history we are taught in our textbooks is accurate (I hope it is), and we must trust that our bank account balance is accurate (I double hope it is), we do not need to have *trust* in the blockchain because we have the liberty to *verify* it at any time because it holds a transparent, unchanging, and immutable record that runs 24/7/365.

9. Open-Source

The label of “open-source” became widely popular in 1998 when Netscape released its source code for the public to see. The software community was very unique in this practice. Unlike any other industry, their incredibly valuable software programs were put out on open forums

for others to study, use, and build upon. It would be the equivalent of Coca Cola putting out their secret formula - something they have fiercely protected for over a century. Perhaps they were not thinking about it with their capitalist hats on, but interestingly enough, software developers were largely a very idealistic group and this decentralized approach to development is one of the cornerstones that enabled technology to grow faster than at any other time in history. The culture of open-source and decentralized technologies is also a cornerstone of Bitcoin.

Bitcoin's open-source nature is not just a "neat" characteristic, but rather it's a design feature that serves several purposes. Like the history of computing technology, Bitcoin benefits from continued innovation since all developers have access to the source code and any promising development proposals can be adopted by the network.

Going back to the concept of "trustlessness", open-source enables anyone to not have to trust a third party - they can simply verify anything about the program for themselves. Decentralization requires open-source code. By anyone having access to the Bitcoin software they can operate a node, create their own wallet, mine bitcoin (support the network) and develop improvements to the code that could potentially be adopted by the entire network.

While some might think open-source code is a security risk to Bitcoin, it is actually a security measure. Those who are new to computer technology often ask the question "How do we know someone hasn't written a bug into the code?" While this is a genuine concern for any centralized software (on which most people operate much of their life, like their bank account or their credit score), this is not a concern for open-source cryptocurrencies. The open-source nature means that the source code is publicly available. In the same way blocks are validated by nodes all over the world, the Bitcoin code itself can be validated by anyone at any time.

Apple co-founder Steve Wozniak spoke of Bitcoin's characteristics in a Yahoo! Finance interview where he stated,

“Bitcoin isn’t run by some company. It’s just mathematically pure, and I believe in nature over humans always.”

When something is good, it can have a spotlight shown on it. Good things thrive on transparency. When something is bad, it wants to hide. Bitcoin’s purity is illustrated by this attribute of open-source. There is nothing to hide, this is a simple concept, but it confounds many people because it’s antithetical to how we are used to the world operating.

10. Secure

The Bitcoin blockchain is the most secure computer network in the world. It is more secure than any government or multibillion dollar company database. How can it be so secure? Bitcoin’s security is derived from its decentralized nature. When Bitcoin was created, it was quite unsecure. It would have been easy to compromise the system but because the network was essentially worthless in terms of dollars at the time, no one cared to attack it. As the network has grown, each new node (computer, phone, device, etc.) that stores the Bitcoin blockchain makes it incrementally more resistant to attacks. Because the nominal USD value of BTC has increased over the last twelve years, those securing the network are incentivized to add further security to protect their now valuable assets.

Charlie Munger (Warren Buffett’s business partner) famously said,

“Show me the incentives and I’ll show you the outcome.”

At the time of writing, Bitcoin miners worldwide make about \$60M per day to secure the network. The amount of newly minted Bitcoin stays the same (cut in half every four years) but as utility and therefore demand increases, the incentives to miners have also increased.

This provides a very high incentive for the existing miners to provide the greatest amount of security possible, but it also incentivizes new miners to plug into the network, thus creating greater decentralization and greater security.

Decentralization is a security feature in that there is no proverbial “off switch” to the network. This is a distinct advantage that Bitcoin has over any centralized (traditional) system. While the NSA or FBI may have very rigid physical security and high-tech firewalls, they suffer from centralization. Even if they store their data in a few different facilities, they are orders of magnitude less decentralized than Bitcoin. Operators within those agencies have knowledge of where those critical locations are, making them susceptible to espionage or sabotage. Bitcoin wins in this element of security as well because while some Bitcoin nodes may personally know the hosts of several other nodes, they have no knowledge of where the vast majority are. This obfuscation is a wonderful byproduct of the brilliant engineering by Satoshi.

To turn off the network you would have to turn off every single node around the world. For all intents and purposes, this is impossible. A massive electromagnetic pulse (EMP) attack would only be capable of taking down portions of the network that would promptly return to normal function and join the rest of the working network as soon as they were able. In the dystopian event of nuclear war where half of the world is destroyed, Bitcoin would still stand. While these are not fun things to think about, they are inevitable quandaries that seem to pop up in the curious minds of Bitcoin-seeking individuals.

With regard to the security of individual transactions, Bitcoin uses an incredibly complex and highly secure cryptographic algorithm called SHA256. By using a public cryptographic key (public address) and a private cryptographic key (private key), users’ identities are protected. Instead of inputting one’s sensitive information into a payment portal online for ecommerce, a Bitcoin transaction consists of the individual simply telling their Bitcoin wallet where they want their funds to go. No personal information, card numbers, etc. is entered so there’s no susceptibility for identity or financial theft.

We don't often think about how unsecure the existing payment systems are. Let's think of it this way: with the existing payment systems for ecommerce, it's like going to buy a hotdog at a park and leaving your credit card on a public bench and telling the hotdog street vendor, "Hey, my credit card is over there. Just go ahead and charge it." With Bitcoin it's like giving the vendor cash directly. In the latter transaction there's no room for a security breach. In the former, you are playing a risky little game by leaving your card information vulnerable. Bitcoin is highly secure on both the micro individual level and the broad macro level. In fact, no system in history can boast of such security.

We will cover Bitcoin's security in greater depth in the next chapter..

Chapter Five: *What Makes Bitcoin So Special?*

“I think that the internet is going to be one of the major forces for reducing the role of government. One thing that’s missing that will soon be developed is a reliable e-cash. A method whereby on the internet you can transfer funds from A to B without A knowing B, or B knowing A.”

- Milton Friedman,
Economist, 1999

We have already discussed some of the novelty of bitcoin and the Bitcoin Blockchain. It’s difficult to discuss it and not marvel at its originality. Some of what makes Bitcoin so special has already been laid out and some points have only been touched on so we will flesh them out further in this section; while other concepts in the section will be fresh in hopes to grant a more robust perspective on the magnitude of the blockchain revolution.

From the 1980s and the pre-internet era to now, the world is almost unrecognizable. Computers, the internet, and the mobile wave of technology have transformed every aspect of life, for better or worse. While this transformation has been incredible, it has also been defined by concentrating power, wealth, and influence. Social media has concentrated narratives. The Fed has concentrated wealth. The elite class has concentrated influence. But with great optimism, I believe the next

ten years will see an even more meaningful transformation brought about by blockchain (Web 3.0/the internet of value) in that it will usher in an era of democratized prosperity. Bitcoin represents the separation of money and state. This technological advancement will grant power, wealth, and influence back to the people ... if we can keep it.

A Declaration of Independence & a Constitution

The Bitcoin whitepaper is both a Declaration of Independence and a Constitution. As a declaration of independence, it represents the first time humanity could declare financial independence in the world's first truly equal financial system. A system free of human biases that does not, and cannot, discriminate based on someone's race, religion, or citizenship. Whether rich or poor, everyone has the same access to the Bitcoin blockchain.

As a constitution, it is a transparent set of rules that everyone can see before they freely choose whether to interact with the network, or not. The United States constitution requires three branches of government to perform checks and balances upon one another to uphold its constitution. While this system has shown to be good relative to other systems, it is still imperfect because of the insertion of humans that are fundamentally flawed. Bitcoin as a constitution works perfectly because the rules are set in stone and reinforced by incentives that align the interests of the participants of the network.

Digital things could be made finite for the first time

This concept is what prompted my Bitcoin "light bulb" moment. I had been fascinated by Bitcoin for some time before, but in early 2014 when I was coming home from vacation, I heard Andreas Antonopoulos speaking as a guest on an episode of The Joe Rogan Experience. I was enthralled. But, when it clicked for me was when I grasped the idea that before Bitcoin, digital things could not be made scarce. Suddenly I realized what a game-changer crypto assets would be. I don't know if this just sounds like a bunch of words to you, or if it's as profound to you

as it is to me. But meditate on that for a moment: digital things could always be easily replicated... until Bitcoin.

In the history of computer science up until Nakamoto's whitepaper, there was no way to disable something digital from being duplicated infinitely. Imagine you're typing in a Word document. Once you write a paragraph, you can just highlight the text and then hit copy and paste. You have just taken digital words and duplicated them. This is hugely convenient in many computer applications, but it's the sole reason why no money or currency could have possibly been digital before Bitcoin provided the solution - no money could ever function if it could just be reproduced by anyone at any time. Even USD isn't this bad. While it can be replicated endlessly by the Fed, at least there's only one party doing this. Imagine if any person in the world could increase their bank account with just a few clicks! Bitcoin's advent was a truly historic moment in this regard.

Key Point: before Bitcoin, digital things could not be made scarce

This point is made a little clearer when we look at the history of some analog industries that became digital very quickly because of the ubiquity of the internet. Let's look at music. I was a highschool student in the early 2000s. In 1999 a company called Napster was founded by Sean Parker (Justin Timberlake's character in The Social Network) and Shawn Fanning. Napster was a music file downloading website - think iTunes where you didn't have to pay.

Why was a company able to share music downloads for free when it would cost millions of dollars to buy physical CD's or tapes to have access to so many songs? Because music had recently undergone a technological advancement. It went digital in the form of MP3 files, and when something is digital, it can be copied and pasted (or downloaded) without limit. While this was one of the coolest things ever for a fourteen-year-old kid that wanted to make a sweet summer mix for free, it most certainly wasn't fair to the artists and record companies that produced the music. When songs could only be released via physical

formats like records, tapes, or CD's, each song or album had monetary value that was controlled by the producers.

Rock Stars were multi-millionaires and record producers created music empires from all the money they made because these songs had so much value. But, as soon as these files went digital and they were able to be replicated endlessly, they lost much of their value overnight. The digital transformation of music caused the industry to change. Musicians make only a fraction of the revenue each time a song is played on a streaming service. Instead of making big money from albums and song plays, they make the bulk of their money from live shows and merchandise (the exact opposite of how their revenue model worked before).

Exponential growth in the field of computer science, the advent of the internet and the mobile technology wave ushered in the digital revolution. Why was it a revolution? Because everything that was once analog, is now digital. Or at least comes in an optional digital form. We already made the case for music, but it goes beyond that. Commerce was once location dependent, meaning you could only shop places where you were physically present. Ecommerce completely changed the dynamics of retail. Entertainment has been digital since the inventions of the radio and television, but with the emergence of computers and the world wide web, entertainment went beyond "regularly scheduled programming". Users could play video games, keep up on their correspondence, play online poker, or whatever else they chose to do for fun.

In its analog form, mail and the postal service was quite efficient. It connected people by giving them the ability to correspond with a relative on the other side of the country in a matter of only a few days or a few weeks. Email enabled that same correspondence to be sent in less than a second. And beyond just sending a handwritten letter and maybe even a photograph, mail going digital made it possible to send text, multiple pictures, videos, pdf documents, hyperlinks to websites and more. Education and conferences have gone digital, and on a personal level, even friendships have gone digital through social media. For better or worse, pretty much everything that was once analog only, now has a digital version, and often the digital version has many advantages.



Everything Going Digital

Things that didn't exist
25 years ago

- | | |
|--------------|-------------|
| Bitcoin | Slack |
| Facebook | Zoom |
| YouTube | AirBnB |
| Instagram | Spotify |
| Twitter | Pandora |
| iPhone | Skype |
| Android | Google Maps |
| Wikipedia | Snapchat |
| iPad | LinkedIn |
| Gmail | Pinterest |
| Netflix | Messenger |
| Amazon Prime | Chrome |
| Reddit | Hulu |
| Podcasts | |

Computer science and the internet have digitized almost every component of our lives, but it wasn't until 2008 that money was digitized. For decades, there were many attempts to do so, but a viable solution could not be found until Nakamoto's whitepaper. It was such a difficult problem to solve because out of all the traditional systems, money and currency are arguably the most important. It couldn't have any holes or flaws. All the previous iterations of digital money had the critical flaw - they relied on trust. They all required a centralized third party, essentially recreating the centralized systems that already existed.

Every single time a digital version of something arises, it displaces its analog predecessor. USD and fiat currencies are analog, and Bitcoin is digital. If I had to place my bet based upon historical precedence, I'm going full send with Bitcoin.

The most secure computing network in the world

Bitcoin is the most secure computer network in history. It is more secure than Amazon web services, the credit bureaus, and even the CIA and FBI databases. The network is so secure for four reasons: transparency, cryptography, decentralization, and sheer computational power. Being the most secure network ever makes it worthy to be the backbone of the world's financial system.

In thirteen years, the Bitcoin blockchain has never been hacked. Sure, individual wallets and passwords may have been hacked because of user error, but the network itself has never been hacked. This difference is worth noting because Bitcoin antagonists will make misleading claims about this. The difference between an individual wallet being hacked and the Bitcoin blockchain being hacked is like thinking that if someone hacks your Bank of America online account that they now control all US dollars in existence. This is absurd, and anyone that makes such a claim is displaying their lack of understanding on the topic.

With regard to Bitcoin's cryptographic security, it currently relies on what's known as SHA256 cryptography. Interestingly enough, SHA256 was developed by the National Security Agency (NSA). SHA stands for Secure Hash Algorithm. The number 256 stands for the amount of bits used in the cryptographic hashes. This equates to a

64-character alphanumeric string (a string of letters and numbers). So, it's not just a 64-character number (with 10 possible numerals 0-9), it also has the added complexity of the 26 alphabet characters (A-Z). The fundamental difference between storing information in a hardware database vs storing it cryptographically is that with a hardware database, although it is digital information, it has a physical location that can be compromised. With cryptography, your data is stored within mathematics itself. Without getting into the minutia of that, let's just leave that at *mind-blowing*.

This cryptographic protection secures every transaction and function on the network which not only protects the transaction, but it also protects individual user identities and bitcoin holdings from any potential bad actors. SHA256 is so secure that cracking its hash is the equivalent of guessing a number between 1 and 115 quattuorvigintillion - that's a 78-digit number (for reference, a billion is a ten-digit number). This means that the chance of accidentally guessing a hash that could unlock someone's bitcoin against their will would be 1 in 2^{256} . For comparison (and kind of a mind-blowing mathematical fact), a deck of cards has 52 unique cards in it. It's mathematically probable that *no two decks in the history of all time have ever been shuffled in the exact same way!* 2^{256} is so much more massively complex than a 52-card deck our minds really have a hard time grasping the magnitude.

Furthermore, if technological advancements made SHA256 insufficient in terms of security, the cryptographic difficulty could be increased as needed. So yeah, it's secure.

The next line of Bitcoin's defense is decentralization. By contrast, centralization is a fundamental flaw in every other secure database. The CIA, for example, is a highly secured system because it houses very important information regarding national security. There are plenty of firewalls, cryptography and other security measures that make it well protected. But it is inherently weak when it comes to centralization. Because the information is so sensitive, it cannot be trusted in the hands of many people at many different locations. Unfortunately, when it can't be entrusted to the hands of many people, only a few places can store the information. This is an attack vector

because bad actors only need to compromise a select few locations to disrupt, destroy, or hack the CIA servers.

Bitcoin's decentralized nature makes it superior. It is estimated there are about one million miners and an additional thirteen thousand full nodes on the Bitcoin network. This means that instead of pulling the plug on a computer to turn off the network, one would need to pull the plug on over one million computers and devices around the world. Keep in mind that these devices are anonymous, and they can be anywhere in the world. These users are technologically advanced as well and likely use sophisticated antivirus protection, VPN's and other protection measures, making *each one* of these nodes very difficult to attack. These points on the network are in different cities, states, countries, and continents, with various geopolitical protections. Some mining locations are in remote desolate areas like frozen tundras where wind power is plentiful and the freezing temperatures keep their mining hardware cool. Some miners are in otherwise uninhabitable places siphoning geothermal energy from volcanoes to power their mining rigs. Bitcoin's decentralization makes even the thought of corrupting the network dizzying.

As if Bitcoin's cryptography and decentralization were not enough, the computational power of the various miners is staggering. Let's say that you wanted to hack the Bitcoin network and you realized that you couldn't break its cryptography and you wouldn't be able to target the nodes one by one because there are far too many of them, you would look to do what's called a *brute force attack*. This simply means that you want to overpower the existing computational power of the network.

Specifically in blockchain, this is called a *51 percent attack* because you would be attempting to have enough hashpower to be greater than 50 percent of the network. In the same way that you only need to own 51 percent of a company to have a controlling interest, you would need to control 51 percent of the network to control the next blocks. While this might sound simple, in practice it is essentially impossible. A 51 percent attack has never been accomplished against Bitcoin. It may have been possible in the early days when the network's hashpower was low, but even then, it didn't happen. This is one of the

critical issues for many other blockchains, even popular ones like Ethereum or Solana. Although these two blockchains are amongst the biggest in the world, they have both suffered 51 percent attacks. Luckily, both attacks were brief, and neither was catastrophic, but these are vulnerabilities that perpetually exist for smaller blockchains but aren't a credible threat against Bitcoin.

To put Bitcoin's hashpower into perspective, it has more computational power than five of the most powerful governments in the world combined. Currently, a coordinated attack by the US, China, Russia, Israel, and Iran would not be capable of a 51 percent attack on Bitcoin, nevermind the fact that some of these governments are enemies and would never collude. And, most likely, since there are governments adopting Bitcoin in some capacity, if there was a coordinated geopolitical attack against the network, these pro-Bitcoin governments would balance the power and tip the hashpower scales back toward decentralization.

Think of a hash as if you were trying to guess a really long number. Computing power is measured in how many of those guesses you can make in one second. Currently, the Bitcoin miners contribute 248 million tera hashes per second (TH/s). A tera hash is one trillion hashes. This means that the computational power of the Bitcoin network is over 248 quintillion hashes (or number guesses) *per second*. For perspective it goes millions, billions, trillions, quadrillions... quintillions. A smartphone mining Bitcoin can produce about 1,500 hashes per second. It would take about 94 quadrillion smartphones to perform a 51 percent attack against Bitcoin. So yeah, the network has some serious power.

One last thought on hashrate wars: keep in mind that Bitcoin operates on Game Theory. This means that when someone makes a move, other participants are then likely to make counter-moves. So, if a bad actor begins adding computational power to the network, they would be increasing the security of the network up until they reach 51 percent. This also means that for other miners to stay competitive and receive block rewards, they would have to add *even more* computational power to the network themselves. What this means for the bad actor is that they have made it even more difficult for themselves to attack the network as

the hashpower would be constantly scaling up, making their attack even more competitive and difficult.

Bitcoin is as much about transparency as it is about security. In fact, transparency is a critical security feature. Why do people put motion detecting security flood lights in front of their homes? Because if there is a would-be intruder, the light would shine on them and expose their bad actions. Transparency has been absent in every financial system in the history of mankind, which is a tremendous financial security threat to populations. With regard to the security of the blockchain, Brian Brooks, CEO of BitFury and former US Comptroller of the Currency, knocked it out of the park in his speech before congress on December 8th, 2021:

“Blockchains are as much about transparency as they are about security. So one of the biggest problems when you think about the biggest cyber attacks that we have had in the United States is how long it took for us to figure out that they occurred. In the case of Target, in the case of Equifax... we found out days and weeks later... by accident that they occurred. When you think about the Equifax one in particular: initially we thought it was a small problem. Weeks later we discovered that it was a medium sized problem and only months later did we learn it was a gigantic problem that involved all of our data. Because there was no transparency. The thing about blockchains is every single block as it is validated is publicly visible to the network. The other thing about blockchains is that it is based on a consensus mechanism. So before you can have a change to the ledger, you have to have a significant majority of all of the validators agree that that’s the correct change. So unlike normal networks where one bad guy can defeat the entire system. Here you have to have thousands of computers agreeing at the same time that the change can be made and even then everyone sees it. That hiding in plain sight is the safest thing about blockchains and is why it’s so critical to our security infrastructure.”

Why is transparency such a powerful security measure? Because even if the impossible happens and Bitcoin's cryptography is somehow hacked, all the miners are located and targeted and then the network is 51 percent attacked, any fraudulent transactions on the network would be visible to everyone around the world. Crimes are only successful when the bad deeds go unseen. But, with Bitcoin, the crime of the century would be immediately apparent to everyone, and remedies could begin immediately.

Aside from Bitcoin's four major protective components of cryptography, decentralization, computing power, and transparency, there are a couple other caveats that make Bitcoin secure. One of these components is understood by looking at incentives. As we have discussed in previous chapters, incentives drive behavior. If a bad actor performed a proper hack against the network, they would need to expend a fantastic number of resources and capital. People would lose trust in Bitcoin if it was hacked in that manner and Bitcoin would lose all monetary value overnight. As a result, there would be no financial reward for the hacker because it would cost vastly more to hack Bitcoin than one would get out of it in stolen value. In the final analysis, there is no financial incentive to hack the network.

Furthermore Bitcoin's open-source nature means that if a bad actor did successfully perform a 51 percent attack and was able to continuously maintain a 51 percent hashpower advantage every ten minutes from here on out (to hack the network for one block would be extremely expensive but to do it in perpetuity would require resources on a level that is difficult to imagine), then the community could simply fork the Bitcoin 1.0 blockchain from the last honest block (from before the attack) and resume operations with Bitcoin 2.0. Everyone's public and private keys would still work for the new chain since it is essentially just a copy of the original chain. It would be like having a digital time machine that could take everyone back to before the catastrophic event. Because would-be hackers know this, it acts as a deterrent from them ever even trying it in the first place.

For all intents and purposes, Bitcoin is unhackable.

It is the first engineered monetary system in history

As we have already established, Bitcoin is the world's first engineered monetary system. This means it was specifically *designed* with good money principles in mind. This was the "unfair" advantage Bitcoin has against all other forms of money - Bitcoin was formulated with *all* of the perfect monetary principles built into it, where other items were simply adopted as money because they held *some* of the characteristics of money. Bitcoin was money made intentionally. Other commodities were only money by happenstance.

As with any other system, it will continue to undergo improvements. If Bitcoin was a baseball game, we are still in the 3rd inning - there's a long way to go. It bears repeating that previous forms of money were stumbled upon, which is the equivalent of a first-time cook making a meal without a recipe and only having a few ingredients (traditional forms of money). Bitcoin, on the other hand, is designer money. This is the equivalent of making a meal with recipes and a fully stocked pantry under the expert supervision of a world-renowned chef.

Bitcoin's attributes beat all analog incumbents of money like gold, glass beads, and Rai Stones. No other cryptocurrency even comes close to exemplifying the monetary qualities of the world's leading digital asset. Even ETH (Ethereum), the world's #2 crypto asset does not attempt to perform the duties of sound money in the way BTC does. ETH functions more as oil for the decentralized application ecosystem. I love ETH and see it changing the world. But it is not money in the sense that BTC is; rather, it is an amazing digital commodity.

Engineered Money: Real Time Cash Finality

While a solid case has already been made for Bitcoin, let's dig a little bit deeper into some of the nuance to get a more robust understanding of what makes this technology so fundamentally important. Bitcoin is the world's first *Real Time Cash Finality Settlement* system. To understand what this means, it's imperative to understand how payments work. One of the most important concepts to understand in payments is the difference between *approvals* and *settlements*. To the

consumer, this may not seem like a very big deal, but to the financial middlemen we are attempting to cut out (Visa, Mastercard, etc.), this is quite important.

When you swipe your credit card in the store you will see an *approval* within a few seconds. This is confirmation to the merchant that your account has the available funds to pay, but no currency is actually being sent at that time. The merchant has essentially received an IOU from your account. The merchant will receive those funds typically in 2-3 business days (this can equate to as many as five calendar days when considering weekends and holidays). When the funds finally exit your account and land in the merchant's bank account, that is a *settlement*.

One may say, "What's the big deal? Aren't they getting the money anyway? Who cares if it takes a few days?" Businesses have learned to operate with this system so it's obviously not catastrophic, but I have been an entrepreneur for well over a decade and have to deal with this process. It requires strong skills in cash management. Blockchain technology will change this. In the not too distant future, the concept of businesses having to wait for up to five days to receive their funds will be an antiquated notion, like thinking travelers should only be able to travel around as fast as a horse and buggy can take them.

Think of it like this: if you must wait for five days to receive payments, at any given time you may be waiting on 16 percent or more of the funds from sales you already made during the month to come in. You have already supplied the labor and the cost of goods to the consumer. So at that point you only have expenditures and no income yet from those sales. Since most companies operate on such small margins, businesses are always looking for a 1-2 percent edge in their operations. In terms of cash management alone, Bitcoin would create a 16 percent efficiency right off the bat. Or look at it this way, even if Bitcoin is running slow that day and takes thirty minutes to process a transaction, the merchant is still getting their funds 96x faster than they would in the best case scenario with existing payment rails where they need to wait at least two days (48 hours divided by 30 minutes). In business, this is a massive advantage.

In my stores, when a customer swipes their card on a Thursday, Friday or Saturday, we do not receive funds until the following Monday

morning. If there is a holiday, it could get pushed back to Tuesday or Wednesday, and this is if there are no issues or hold ups with the banks. In my small businesses, sales across three days will be in the tens of thousands of dollars. While we've provided tens of thousands of dollars worth of services and goods at that point, we must wait to be paid for them. This also means that we need to have additional capital in our accounts for no other function than to provide a bridge from when we render services to when we get paid for them. As a business owner, this feels like an inefficient use of capital.

Imagine what this means for a massive retailer like Walmart. Based on their average sales volumes, it is estimated they have to wait for approximately \$3B in payments to come in during this 48 hour latency window. Imagine having sold \$1.5B of products out of your inventory while you wait for the \$3B (assuming a 50 percent markup on those products) of revenue for those products to come in? Making so much money might sound like a good problem to have, but from a cash management perspective, it's a nightmare. For Walmart this means they need to hold at least an additional \$3B in cash at any given point just to float this slow process! For a company that is incredibly efficient with their use of capital, this must be a frustrating fact.

Bitcoin solves this problem by offering *real time cash final settlements* - this means that instead of an approval and a later cash settlement when a payment is made, the value is transferred immediately. Voila! It's done. On a global scale this means that trillions of dollars won't be stuck waiting for settlement. Instead those monies will be increasing the velocity of working capital and greasing the wheels of industry. That translates to more innovation, more jobs, more wealth, and less poverty.

Engineered Money: Self-Custody, Be Your Own Bank!

Bitcoin enables individuals to be self-sovereign over their own money. Traditionally, banks have been the go-to option for people storing any material amount of savings. Sure, one might keep some extra cash in an old shoebox or in the cookie jar, but people hold the majority of their

savings in banks. It has been this way for centuries. This was certainly a better option than storing all your wealth under the mattress where it was vulnerable to theft or an act of nature that would destroy your savings in an instant.

Storing currency at the bank has worked for most of us, but it does not allow individuals to be sovereign over their own savings. This has been evidenced by the various bank runs throughout world history where, in times of crises, people lined up in front of banks hours before they opened so they could withdraw their funds. They did this because they were unsure whether the bank even had enough liquidity (currency in reserves) to pay all its customers what was rightfully theirs - we will see later that the answer to this question is always “no”.

Banks have evolved along with the internet to some degree and now provide digital interfaces and websites for greater efficiency for their customers. This makes for easier access to their funds and a quick and simple way to check account balances. But, while this has been great for customer satisfaction, it doesn’t mean customers are sovereign over their money - they are still beholden to the whim of the bank. Gold, silver, and cash all enabled individuals to have complete control over their own funds, but in the 21st century, it is imperative that there is a digital option. Bitcoin represents the world’s first digital currency, but it also represents the world’s first digital self-sovereign form of money.

It is worth noting that this is only true for Bitcoin users that use a non-custodial Bitcoin wallet. If one keeps their BTC on an exchange or with any other type of third party (such as a lending platform like BlockFi or an exchange like Coinbase), there is no difference between that and using a traditional bank as far as the control of your digital assets. For a crypto user to be in full control over their money they need to be the only person with their private key. As I mentioned earlier, “Not your keys, not your crypto.” You may have paid for the coins, but if you share your private keys with others, they have the same access to the funds that you do.

Some crypto holders will inevitably choose to store their wealth with one of the numerous banks that are beginning to custody digital assets. They may simply feel more comfortable with traditional methods. That is their choice, but they should understand they are forfeiting one of

the most important features of Bitcoin - the ability to store your wealth yourself.

The rest of us, we experience a tremendous sense of financial liberty by being able to have total sovereignty over our money without being beholden to the institutions we formerly entrusted our savings to. In the US, we currently do not fear the government or banks draining our accounts overnight because we are historically a society of law and order. Around the world and throughout history, this has not been the case for the vast majority of people. There are many instances, even in recent history, where South American and African dictators have taken over a region and commandeered the conquered people's money.

For those who do not fear these major events, they may still not like the policies and regulations of their bank. Overdraft fees, annual fees, high transfer fees and minimum account balances hurt the poorest among us. Limited business hours can be frustrating for customers. Where banks are largely limited to 9am-5pm hours of operation and closed on Sundays, Bitcoin functions 24/7/365. Even with online banking and some after-hours functionality, try sending an international wire through your online bank account at 7pm. It just won't happen. With Bitcoin, you are in control of your funds. Send them where you want. Store them where you want. That is for you and you alone to decide.

When discussing this idea with a physicist and economist, he objected by saying he couldn't see the masses wanting to hassle with securing their own funds, nor would they be comfortable with the responsibility. He might be right. Many people will opt for centralized entities to secure their BTC. This does not mean BTC holders totally lose sovereignty. The fact that one has the *choice* to self custody or a third party is evidence of one's sovereignty over their money.

Engineered Money: Money, Democratized

Bitcoin is money of the people, by the people, for the people. This is important because to this point, all of history's financial systems can be defined as monarchies. While some real life monarchs were benevolent, others were tyrants. This same point is true for traditional

financial systems. While all were centrally controlled by the governments of their day, some worked more freely, and others were designed strictly as a form of control over the population. Regardless, Bitcoin represents a new concept in systems of finance: equality. Traditionally, those that controlled the currency printing press controlled the economic, and often, political system. Directly under that group was their gaggle of cronies who were the first to get access to freshly printed currency and therefore have a major advantage over the rest of the population.

There will always be wealthier and poorer individuals. Some people will be better with money than others. Some start life higher up or lower down in the socio-economic order. Some people are obsessed with building wealth while others want just enough to provide for their household and spend their time enjoying life. The goals of individuals vary, and this will always provide a distinction between those with more or less wealth. But it is worth noting that historically, the life choices made by individuals are not the only factor that determine rich and poor.

Traditional financial systems were developed with the scales tipped. Those building the systems always designed them to benefit some and disregard or even suppress others. Those wanting to build wealth or provide for their family were often crushed by unofficial class systems that prohibited them from building wealth. Their labor enriched others and provided only a subsistence lifestyle for themselves. This is a point where both the politically left leaning who have railed against the financial establishment for some time, and conservatives who often vote to uphold the status quo (I believe mistakenly so in this instance) agree.

Allow me to give one such example of how these scales are tipped. Under United States regulations, all investors do not have the same rights. Yes, anyone can invest in the stock market. But the most lucrative of investments are withheld from the general public. There is such a thing known as being an “accredited investor”. In order to be an accredited investor, one must have an income over \$200,000 per year and a net worth of over one million dollars. US regulators say that these individuals are allowed to invest in a wider array of investments because they are more financially resilient in the event of a risky investment

failing. The concept of accredited investors was created under the guise of “protecting the little guy”.

This begs the question, if the government is so concerned about protecting poorer individuals from risky financial endeavors, then why do 45 of the 50 US states have government sponsored gambling in the form of lotteries? Lotteries do not enrich populations. Quite the opposite. They are another form of taxation that predominantly targets the poor. Investing, on the other hand, is a practice that has historically shown to enrich populations and yet, there is government sponsorship of the former, and government prohibition of the latter. This is one such example of what I mean when I say that the scales are tipped.

Imagine the financial system as a casino. Us regular people are the gamblers in the casino. The odds of every game are tipped in the favor of the casino - basically, the system is rigged, and everyone knows it. The gamblers may win sometimes, but ultimately the house has the advantage. We don't want to be the gamblers; we want to be the house. When you put your money in your savings account with the bank, what do they do with it? They give you 0.01 percent interest and lend your money out to someone else at 7-20 percent interest.

Bitcoin and Decentralized Finance (DeFi), built on top of Ethereum, provide a technological solution so that for the first time ever, regular people can be the house. With DeFi, you can lend your bitcoin or another cryptocurrency via a smart contract and because there is no bank to be the middleman, you earn that sweet 7-20 percent interest. Instead of your bank making money with your capital, now you make money with your capital. This is the fundamental difference between the wealthy and the poor - the wealthy have learned to use their capital like it's an employee that works for them. For the wealthy, their capital *always* generates a yield (interest).

With DeFi, the individual with any kind of savings, big or small, is no longer just a *saver*, they are an *investor*. As the saying goes, “The poor spend, the middle class saves, and the wealthy invest.” DeFi enables even a meager savings to be used to generate yield and provide a second source of income. Participating in DeFi just means you are either a direct lender or a direct borrower. If you need access to capital, you can borrow directly without a credit check. If you have some money saved and you

want to earn interest, you can use a smart contract on Ethereum to lend out your money to generate interest rates that are far superior to a traditional savings account.

This means that the single mom who works two jobs to provide for her children need only to put any little bit of excess money she has to work, and it will instantly be like she has a third job. This third job will only provide a small revenue stream but, because of the power of compounding interest (what Warren Buffett calls the 8th wonder of the world), if she remains diligent in thinking like an investor and continues to put her capital to work, that third income will become substantial and will completely change her family's financial future. With a 0.01 percent interest rate in a savings account from her bank this simply isn't possible. Because she had so little capital to begin with, she would not be allowed to invest in anything that would generate any significant return. DeFi enables that mother to participate in a system that benefits her as much as it benefits the millionaire investor that started the game on 3rd base.

Furthermore, Bitcoin and Decentralized Finance represent a quantum leap forward in financial technology and have an unprecedented ability to bank the unbanked. An astounding 31 percent of adults around the world are unbanked⁽³⁾. That means over 1.7B adults (and therefore many more children) do not have a bank account. Many more are underbanked. Lacking a bank account cripples the ability of those individuals to participate in their country's economy beyond their own local micro economy, and they are even less able to participate in the global economy that would give them access to wealth and prosperity. This is because these parts of the world sadly have so little wealth already that it is not profitable for banks to provide services in those regions.

What's so amazing about Bitcoin is that it is already beginning to bridge this gap for the unbanked and underbanked. Anyone with a smartphone or an internet connection can immediately be their own bank by using the blockchain. Skeptics might say, "These people are too poor to have a bank account but they somehow have a smartphone? I doubt it." Well, that doubt would be ill-founded. Smart devices, WiFi and the internet are ubiquitous in some of the poorest communities around the world.

It's a pretty wild thought to ponder how people in El Salvador went from having limited banking access and just skipped right to the blockchain. But poorer countries actually have a history of skipping certain eras of technology. For example, countries like Zimbabwe largely never had landline telephones because there was a tremendous cost associated with building that infrastructure. So many Americans who travel there are shocked to see everyone walking around with a smartphone. This technology skip happened because it was much more efficient and cost-effective to build out a mobile telecommunication network than a landline network.

Since blockchains do not have a central authority, there is no one to tweak the system to tip the scales in their favor. The fact that blockchains have a predetermined set of rules (found in their whitepapers and verified by auditing the code) allows individuals to choose to interact with whichever blockchain they choose. If someone doesn't like Bitcoin, they can choose to use Ethereum or XRP or one of the other twelve thousand blockchains. But not all blockchains are created equally. Bitcoin has the most users, and therefore the most votes of confidence, largely because it has the most just and equitable set of rules.

Even if Satoshi Nakamoto resurfaced some day and decided that he wanted to access his one million bitcoin, he would have no more authority or power over the network than you or I do. Bitcoin does not care if you are American, Lithuanian, Russian, Chinese, Israeli, or Palestinian. It does not care if you are Christian, Muslim, Jewish, Buddhist or atheist. It does not care if you are Green Party, Democrat, Republican or Libertarian. It does not care if you like the Yankees or the Red Sox. Bitcoin is the first inclusive financial system that grants the same access to the poor mother and father in a developing nation that has a thousand sats to their name that it grants to billionaire Michael Saylor who holds well over one hundred thousand entire bitcoin. Existing financial systems pick winners and losers. Bitcoin does no such thing. If Bitcoin did not provide this fair and equal access, people could vote against it by no longer using it. But, because the network is growing exponentially, fresh votes for a new financial paradigm are coming in every day. It is money democratized.

Green Bitcoin

I'm going to make a shocking and inflammatory statement: Bitcoin is the key to a sustainable green future.

This is quite possibly the most misunderstood aspect of Bitcoin. Famous politicians in Senatorial and Congressional hearings have parroted phrases alluding to Bitcoin being bad for the environment. They say things such as, "Bitcoin consumes as much energy as a small country." First off, small countries don't require much energy so that is a very low bar. While it initially sounds problematic, this is an overaggrandized comparison. Americans use vastly more electric power for their Christmas lights in a single month than small countries like Ireland or Ethiopia use in an entire year⁽²⁾. I will elaborate more on these statements from politicians and "experts" in the *Short Answers to Common Questions* section later on. For now, I want to focus on the positive and support this bold statement about *green Bitcoin*.

I am not alone in this estimation. Cathie Wood, the CEO and CIO of Ark Invest, a \$50B investment fund, is a well-known voice who agrees that the financial incentives of Bitcoin will enable renewable energy sources to be built at scales necessary to provide consistent and reliable power. Cathie Wood is well known for her forward thinking in regard to her investment strategies and her calls for substantial investments in Tesla and other tech companies that have netted incredible returns, outperforming the rest of the market.

A challenge with renewable power facilities (specifically solar and wind) is that they should be overbuilt to be able to handle peak capacity, but it isn't cost effective to do so. Imagine for a moment the limitations of a field of solar panels that power a city. The shortcomings of solar farms are well-known. They are costly to build, susceptible to bad weather, and solar energy is only present for certain hours of the day. This means that many solar fields are underbuilt because otherwise they will be too costly for the potential savings they can actually return.

If a solar farm is overbuilt to accommodate peak demand, when there isn't enough demand at off peak times, which is often, much of the

solar power would be pure waste. Batteries are not currently efficient enough to be a viable solution to this problem. And since solar panels have a lifespan 25 years at peak efficiency, they need to make a significant financial return before they are decommissioned. There is much working against the mainstream adoption of solar. Enter, Bitcoin.

How can Bitcoin be the solution to this problem? Simple, Bitcoin provides a financial incentive for solar farms to be overbuilt to accommodate peak demand. Any excess energy that the farm produces in off peak times can be diverted to highly profitable BTC mining. This just means that if you were producing 1,000 kWh from your solar farm, but your city only needed 500 kWh, you could divert your excess 500 kWh power by flipping on your BTC miners. Because battery technology is not efficient for long term large storage, under the current system, that 500 kWh of clean energy would be completely wasted.

At the time of writing, the most efficient miners can mine a bitcoin at an average cost of \$5,000-\$7,000 per coin. Considering that BTC is currently worth about \$50,000 this is a highly profitable venture. When you consider that the biggest expense for miners is their electricity cost, then you see the tremendous value proposition of using excess *free* energy to mine bitcoin at an almost pure profit.

Another area where Bitcoin is already improving the environment by eliminating pollution is in the fossil fuel industry. A gas flare, also known as a flare stack is a gas burning device used in industrial plants such as petroleum refineries, chemical plants and natural gas processing plants. They are also common at oil or gas extraction sites such as oil wells, gas wells, offshore oil and gas rigs and even landfills.

In industrial plants, flare stacks are primarily used for burning off flammable gas released by safety valves during unplanned over-pressuring of plant equipment. During plant or partial plant startups and shutdowns, they are also often used for the planned combustion of gasses over relatively short periods. At oil and gas extraction sites, gas flares are used for a variety of maintenance, testing, emergency, and safety purposes. In a practice known as *production flaring*, they are also used to dispose of large amounts of unnecessary associated petroleum gas, throughout the life of an oil well.



The amount of toxic pollution and carbon emissions that get pumped into our skies from this feature are enormous. It's an unfortunate side effect of this type of energy production. But necessity is the mother of innovation. There are BTC miners who have developed a novel business around hooking up mobile mining rigs that harness the power of the gas flare and, rather than burning it and polluting, use it to mine BTC. This process actually makes Bitcoin a net negative carbon producer. The financial incentives provide these otherwise polluting companies a self-serving option to do what's in the best interest of the environment. What a beautiful free market solution!

As if the case weren't already strong enough for green Bitcoin, let's go one step further. Quite possibly the most bizarre-sounding solution in the pursuit of producing environmentally responsible energy is the harnessing of geothermal power - in other words: using volcanoes or other natural heat sources to generate electricity. While this might sound like science fiction, the country of El Salvador has already begun plans to mine BTC using their volcanoes. Volcanoes provide tremendous amounts of geothermal energy that is untapped by civilization, and this is for good reason. Most people don't want to live near a volcano.

This brings up one of the most profound aspects of Bitcoin and why it will be so revolutionary. For the first time in history, energy production is not location dependent. Meaning, that where you produce energy does not need to be in close proximity to civilization. Aside from the high infrastructure cost of running power lines over vast expanses,

energy is diffused over such distances. This means that the transportation of energy is not cost or energy efficient. Bitcoin allows remote power facilities to be built and to transfer value from areas with the ability to generate high amounts of electricity that are not habitable. This opens areas with remote waterfalls and other natural features that can produce clean and sustainable energy across the world. This is yet another game changing attribute that helps stamp the pro-Bitcoin case.

Gas flares, solar farms, remote waterfalls and volcanoes - these solutions might sound strange, but they are profound, and I believe history will look back on them fondly. If one of the biggest hurdles for the mass adoption of wind and solar farms for the purpose of generating power for cities was their lack of economic feasibility, then mining BTC with their excess power means that Bitcoin was the missing piece necessary to transform an entire industry. I believe we will see an explosion of clean renewable wind and solar facilities where Bitcoin will be at the heart of their operations. As history has shown, many of the early accusations against an emerging technology actually end up being the exact opposite of what actually happens. To say that Bitcoin is a net negative for the environment is usually only uttered from a lack of understanding or by those with conflicting motives. What a turn of events it will be to see Bitcoin as the economic key to a cleaner planet.

The First Public Service Not Provided by Government

In a democracy, or more specifically, a Constitutional Republic as we have in the United States, the idea of a public good or service is, *in theory*, provided by the people. The government is essentially supposed to be a representation of the people. So, things like public schools or public roads are services provided by the people, for the people. But the experience of most individuals is that their government is not always a perfect representation of themselves. In fact, their school board, city council, or state representatives may be acting in a manner that is contrary to the will of many of the people.

A public good or service is, *in practice*, something that the government provides for its citizens. And often, in practice, the government has become its own entity separate from the people. Bitcoin is revolutionary with regard to it being the world's first public service that is provided directly by the people without the need of government intervention. Any establishment career politician may shudder at this realization. This doesn't mean that blockchain makes government obsolete. What it does mean is that now there is a third sector in addition to the public and private sectors. This is a new hybrid sector that can be thought of as *decentralized commons*. It is run by private individuals acting on their own volition to provide a public service for anyone to use.

As we discussed earlier, this public service enables everyone to have access to financial services. Those that have never had access to a bank can now be their own bank; provided by the community. We might think of only those in developing nations as the unbanked, but you might be shocked to know that, according to the FDIC, six percent of US households are unbanked⁽⁴⁾. That's a total of 14.1M American adults. For these households it means perpetuating cycles of poverty from generation to generation. These households now not only get to access financial services, but they can also participate in a system that can enable them to climb the socioeconomic ladder.

Furthermore, one of the chief mandates of government is to secure the property rights of its citizens. This means that if someone owns something, the government will protect their ownership. If someone tries to take ownership unlawfully, they will send men and women with guns to stop it. If a thief has already stolen that person's property, they will return it to its rightful owner and punish the individual that stole it.

Most people are familiar with Thomas Jefferson's line regarding inalienable rights being "life, liberty, and the pursuit of happiness" but fewer people know that Jefferson adopted this concept from British political philosopher John Locke. Locke was famous for the phrase, "life, liberty, and property." This concept of the preservation of property was a core concept to the founding fathers of the US. It was viewed as a cornerstone of a free society. Jefferson believed that the pursuit of happiness came with the understanding of property rights built into it.

Until 2008, aside from government, there was no public service that could preserve an individual's property rights. While those in America may take this for granted, many abroad will find this revolutionary. Bitcoin is the world's first public ledger of property rights (currently in the form of BTC but new innovations are happening in blockchain that mean individuals can secure all sorts of property rights this way). Aside from a twelve or twenty-four-word seed phrase you have no other requirement to secure your BTC property. There is no tax, annual fee, or city council meetings that you need to attend to secure it. Your freedom to secure property via the Bitcoin blockchain is your birthright as a sovereign individual.

Developed nations may find this less profound, but imagine you were a Polish Jew during WW2. It took only thirty-five days from the time Germany invaded Poland until the country was completely conquered and occupied. Hardly enough time to sell belongings and make appropriate preparations to flee. Polish refugees immediately lost any protection of property rights when they were under foreign rule because at that time, property rights could only be secured by the government, and their government no longer existed.

Had Bitcoin existed in 1939, Jewish Polish refugees would still have had many dire issues but maintaining their BTC property rights would not have been one of them. And the ability to have financial resources was the difference between life and death for many thousands of families.

Under the globalist monetary policies of the International Monetary Fund (IMF), the small country of El Salvador became dependent on international loans. These loans never enabled them to get ahead. The old paradigm simply kept El Salvador dependent and poor. The vast majority of El Salvador's citizens were unbanked, even after having worked with the IMF for years. Only 30 percent of Salvadorians were banked. In 2021, El Salvador went on the Bitcoin Standard and made BTC legal tender. Within only four months, 60 percent of Salvadorians had financial banking services through Bitcoin. What the IMF's old guard approach took years to do, Bitcoin doubled in a little

more than a business quarter. What this means is a path to prosperity for Salvadorians that didn't previously exist.

Providing a public service for the good of all citizens of the world is not a globalist ideology. It's a remedy to help the average person become resistant to encroaching globalist policies. Not only is this public service providing an equal opportunity to everyone for the purpose of banking the unbanked, but it also provides public protection of an individual's property, and thus makes the American Dream a reality in keeping with the essence of John Locke's influence of life, liberty and property - not just for Americans, but for individuals, young and old, rich and poor, around the world.

Fastest growing technology & fastest growing asset in history

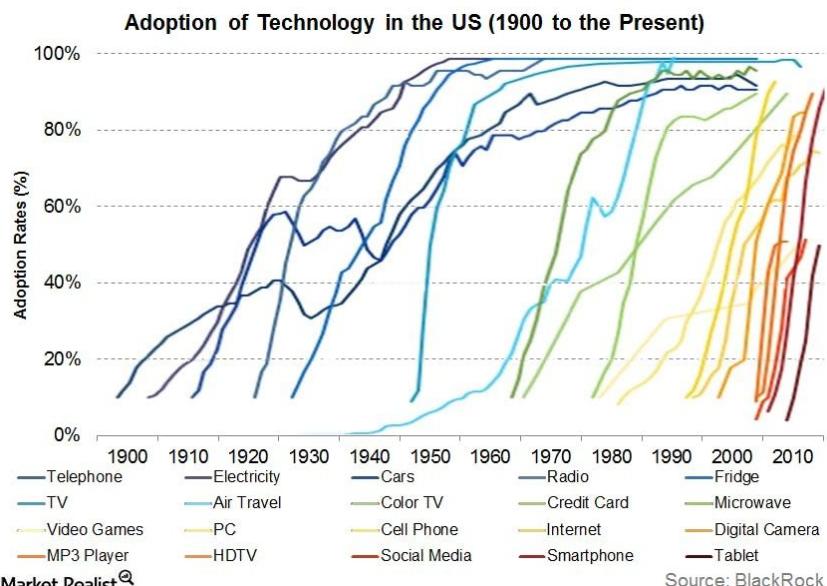
If some of the other geeky attributes of blockchain do not impress you, then maybe the sheer speed of adoption will. It is interesting to note that technology is inherently deflationary, meaning it becomes cheaper over time. For instance, a 50-inch plasma TV in 2000 cost \$20,000. By 2005 it cost \$4,000 and by 2020 Ultra HD 4K TV's (much better quality than plasma) cost less than \$1,000. Technology also tends to speed up the rate of adoption of subsequent technologies (see chart below).

So, it's not surprising that blockchain, being one of the newest technologies, is the fastest growing. But I would posit that it is becoming adopted so quickly because of its importance and necessity. Other technologies increased convenience or provided entertainment while Bitcoin and the ability to send value is an essential part of the human experience. This makes it easier for individuals to recognize its importance and therefore adopt it. Some have and will adopt blockchain because they see its potential as an appreciable asset - this is the most alluring component for many people.

Regardless of how people come to blockchain, they are participating in the fastest adoption of a technology ever. In its first twelve years, the internet grew to 16M users⁽⁵⁾. In the twelve years since the creation of blockchain, over 106M people have adopted it⁽⁶⁾ - a 562

percent greater adoption rate than the internet! And think of the difference in the quality of these adopters. Someone that adopted the internet in the early days may have been someone that simply visited a web page - an action that required almost no commitment. These 106M Bitcoin adopters are people who have placed some sort of financial commitment into the system. Bitcoin's blazing adoption rate is a pretty strong argument against those that say blockchain is going to zero. Imagine in 1995 (but knowing what you know now) having someone say to you that the internet is going to zero; you would laugh at such a silly statement. So, it's a logical conclusion to assume that blockchain, being almost ten times bigger and having users that are financially invested into the protocols as opposed to fickle users, isn't going anywhere but up.

What makes the blockchain adoption story so compelling is that, with the internet, individuals did not have the option to buy part of the protocol. You couldn't buy bits of the internet. You could buy internet company stocks, but that is something different entirely. With Bitcoin and blockchain, you have this unique ability to buy a portion of the protocol itself. Imagine how lucrative the internet would have been as an investment if it only had 21M pieces and you could have bought some of those back in 1995?



No asset in history has grown as fast as Bitcoin. Even without counting the blockchain industry as a whole, Bitcoin itself is the fastest growing asset by market capitalization of all time. No asset or company has reached a valuation of \$1T faster than Bitcoin. As if that weren't a shocking enough statistic, let's go one step further. Even the world's preeminent currency, the US Dollar, took 200 years to reach a \$1T circulating supply⁽⁷⁾!

Wall Street tends to value investments based upon two aspects: adoption by users, and fair market value. Billions of dollars of capital are deployed toward businesses that can exhibit either one of these qualities, even if they display them at a much smaller scale than Bitcoin. But Bitcoin and blockchain win over every other protocol, technology, asset, or company in history in both adoption and fair market value. The importance of this cannot be overstated.

The Current System Is Just IOU's.

People think that prior to Bitcoin, money was already digital because they see their online bank account represented digitally. Or perhaps others believe their money is digital because they can send money to a friend via Venmo. These assumptions are incorrect; this entire system is all just a bunch of digital IOU's.

For anyone that is a millennial or older, I'll ask you to recall the scene from Dumb and Dumber where Jim Carey's character Lloyd Christmas has spent all of the ransom money that the bad guy was supposed to get. With a gun pointed at him, instead of giving the bad guy his \$5M back, Lloyd opens up a briefcase with no cash and only slips of paper with handwritten notes on them. He attempts to pacify the kidnapper by saying, "That sir, is as good as money, those are IOUs. You might want to hold onto this one," and he hands the bad guy a napkin with the words "IOU: \$275,000" written on it for the Lamborghini that he just bought.

You can see how displeased the kidnapper is at the thought of an IOU as opposed to actual stacks of \$100 bills. This is obvious and intuitive, but I'm bringing it up because it illustrates that IOU's are a poor substitute for real value. IOU's require a lot of trust. Our financial

and currency remittance systems function in largely the same way as that briefcase of IOU's.

Physical bills only get settled periodically because of the high cost associated with doing so. Imagine how difficult it would be for banks and money transfer companies to constantly take truckloads of bills back and forth to their counterparties. Do they do this hourly? Nightly? No. They do it much less frequently because they financially communicate with one another via IOU's - Bank A owes Bank B \$1M, Bank B owes Bank C \$3M - and all of this is only recorded on their internal ledgers. The stacks of cash change hands much less frequently. I will elaborate on how this backend process works later.

To the users of Venmo, it looks like their payment is being sent instantly, but what is really happening? Is Venmo taking an armored truck from your Wells Fargo bank branch with the \$8.95 going to your friend's Bank of America branch for the latte they spotted you for? It doesn't take a rocket scientist to see that this would be totally inefficient. So, what the payment processors and financial service companies do is transmit IOU's among one another. Their books update individual account balances in near real time, but the actual funds are only physically settled periodically (monthly or quarterly) because of the excessive amount of effort it would take to move that amount of paper bills.

The President of PayPal (parent company of Venmo), Dan Schulman, famously remarked that although these apps have beautiful front end user interfaces, banks and money remittance companies have been running on early 1970s technology (ACH and Swift). Innovations came in the form of user experience but provided no technological efficiencies on the backend for these companies. By adopting blockchain technology, these companies will see their first real step forward in transmitting value in fifty years. Current users of blockchain for transmitting value have already adopted a more efficient system than what these multi-billion-dollar companies use - this really is power to the people.

It's Going to Be Bigger Than the Internet

Imagine you have a time machine and can go back to 1800. You present a stranger from that time with two different inventions. The first is a box with a button where, when you press the button, it can send a message anywhere in the world. The second is another box with a button, only with the second box, you can send money anywhere in the world. This stranger will be confounded by both seemingly magical instruments. But, if you were to ask him which invention was more important, he would likely answer the latter.

If the internet is the first button, then blockchain is the second.

The ability to send information across the continent with the advent of the US Postal Service enabled people to communicate at a speed and across a distance that had previously been impossible. Sending messages allowed people to stay in touch and even communicate potentially vital information. But it wasn't until the famous Wells Fargo bank wagons trekked across the United States that cities and industry were able to be built. The movement of money made large scale settlement and development possible. Without the transmission of value, resources and labor were difficult to come by. Being able to send money quickly and efficiently allows for new frontiers. Sending information is good. Sending money is even better.

The early developers of the internet protocol HTTP attempted to build a native payment layer to the internet. Most people know that when you go to a broken website link that you will get an "Error 404 (page not found)" response. What many people do not know is that there is also an "Error 402 (payment required)" code in the programming. Early internet developers knew that for the internet to reach its full potential it would need a payment rail. Unfortunately, no such proper digital asset existed at the time.

Web 1.0 was the "text net", Web 2.0 was the "content net" or the "social web". Web 3.0 will be the internet of value. The internet and blockchain will become one and the same. Being able to transmit value peer to peer means individuals will have access to financial tools that were previously only available to the privileged. Web 3.0 enables

individuals to create digital ownership of any of their assets and use those assets as forms of payment. Imagine if you could turn the ownership of your home into fractionalized ownership via coins. A retired individual could pay for their cup of coffee, their groceries, or medical bills with their “house coins”. Anything and everything that has value will be capable of being spent or bought with ease.

This all might beg the question, what will be digitized? Some of the most obvious are stocks and ownership rights for other things like land, collectibles, and intellectual property. Some of the more interesting capabilities of the blockchain for the liberty minded are things like voting rights and personal data.

The blockchain’s inherent nature of being open and transparent makes these use-cases a shoe-in for widespread acceptance. Because they are encrypted, secure and private, individuals do not have to trust in their voting systems, they can verify the results for themselves. Projects such as Civic have begun development in this field and may be the key to ensuring the continuation of trust in democracy. A verifiable and secure voting system maintained on a transparent, open-source blockchain ledger could restore faith in our democratic elections.

One’s personal data will be owned by them and them only. There are already forward-thinking projects like Basic Attention Token (BAT) that have been around for several years. In the traditional model, an app user signs away their right to their information through lengthy terms and conditions. This is how internet companies provide seemingly “free” services; they sell users’ data. Each time that user sees an ad, the social media app they are using gets paid. BAT turns this model on its head. By allowing the user to own their own data, individuals can choose to view ads or not. When they do view ads, they get paid, not the internet company. Using BAT is as easy as downloading the Brave Browser and using it like you would use any other browser.

A native currency for the internet seems almost like it was a prophecy of the early internet developers that is actually coming to fruition. Blockchain was the missing piece that the early developers of the internet protocol were missing. In the same way that bank wagon caravans transmitted value across distance and made thriving societies possible on the new frontier, likewise sending cryptographic value will

make new frontiers possible in a digital world. And these frontiers will be defined by inclusion, equality, and a technologically enabled level playing field.

Make Bitcoin, Not War

Bitcoin is secured by computing power. All financial systems before Bitcoin were secured by might - guns, bombs, and war. Bitcoin flips the concept of security on its head. Whereas all previous systems were secured by militaries (whoever had the greatest offense), Bitcoin derives its security by having the greatest defense.

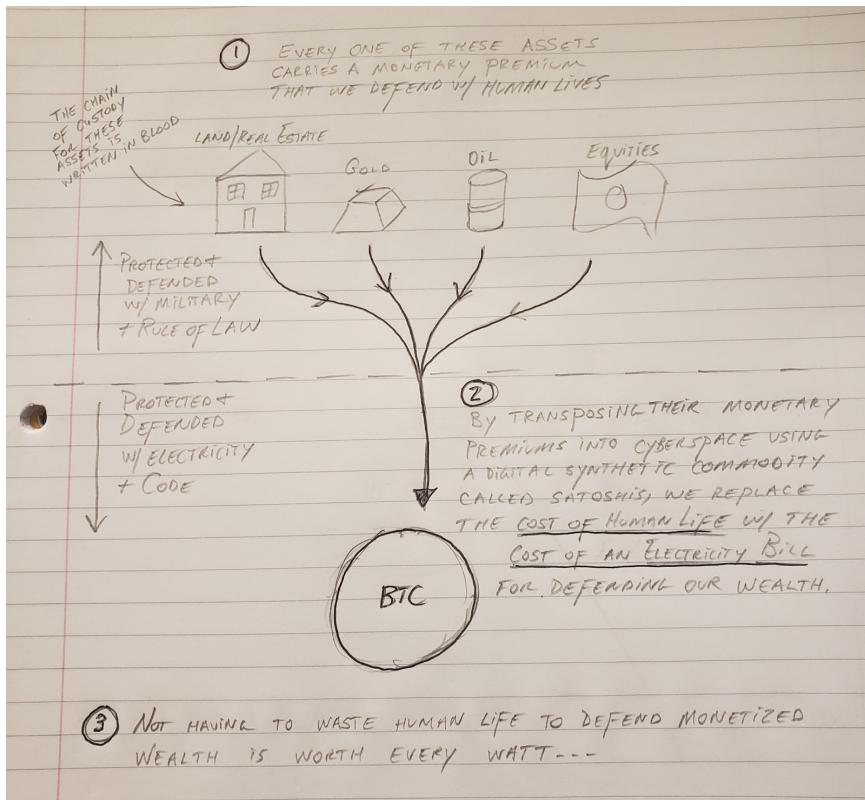
Side Note: I originally wrote this section in December of 2021. I am wrapping up the writing of the book in March 2022. In February of 2022, two major geopolitical events happened: The Canadian trucker Freedom Convoy and the Russian invasion of Ukraine that illustrate this point perfectly. In the former, the Canadian government froze the bank accounts of protestors and donors, the protests were able to continue because BTC donations began pouring in.

Similarly, during the Russian invasion of Ukraine, for the first time ever, a sovereign nation solicited international donations to fund their national defense via a Tweet with their BTC address listed. Tens of millions of dollars began pouring in from all over the world. Whether it was defending freedom of speech or defending the sovereign borders of a nation, BTC has proven to be an incredibly powerful defensive tool.

In a March 2022 Senatorial Hearing, US Senator Cynthia Loomis interviewed Michael Chobanian, the founder of Xreserve, the Ukrainian crypto exchange responsible for accepting donations to the Ukrainian defense. In that interview, Senator Loomis asked Chobanian how long it took them to set up the necessary infrastructure to accept BTC donations from all over the world. He said:

“Bitcoin took about 10 minutes to start accepting donations and was available immediately for use. Accepting Fiat donations through wire transfers would’ve been unable to be used for at least 10 days.”

Securing financial systems by the military essentially meant that you secured your system with human lives. I think most people are in agreement that we would rather spend electricity than the lives of our young men and women.



Tweet by @jasonplowery,
November 1st, 2021

If we look back at the history of the many wars throughout time you will find a common thread - financial motivations. Wars are almost always started for some sort of resource, whether it is land, oil, gold, slaves, or other commodities. If not for resources, then there tends to be

some sort of economic element at its heart. Even ideological wars like the Cold War (Communism vs Capitalism) were economic by definition.

Most Americans learned that “taxation without representation” was the match that lit the fuse of the American Revolution. While that indicates an economic policy was at the heart of the conflict, according to Benjamin Franklin, it had even deeper fiscal roots.

“The colonies would gladly have borne the little tax on tea and other matters had it not been that England took away from the colonies their money, which created unemployment and dissatisfaction. The inability of the colonists to get power to issue their own money permanently out of the hands of George III and the international bankers was the PRIME reason for the Revolutionary War.” (emphasis mine)

This sentiment is echoed in the famous quote by George Washington where he bemoaned the tremendous inflation that was being experienced in the colonies.

“A wagon load of money will scarcely purchase a wagon load of provisions.”

Contrary to popular belief, inflation prompted by an oppressive monarch and banking policies was the primary cause of the war that led to American independence. Broken economic systems have always led to revolution of some kind.

Similarly, most Americans think that their Civil War was fought over the noble mission of ending slavery. While this was a fantastic byproduct of the war, and as the war progressed it became a chief reason to win the conflict, it was not the original reason for the war. By no means do I want to tarnish the reputation of Abraham Lincoln, but soon after his inauguration and right before the first shots of the war were fired, President Lincoln declared⁽⁸⁾,

“I have no purpose, directly or indirectly, to interfere with the institution of slavery in the states where it now exists. I believe I have no lawful right to do so, and I have no inclination to do so.”

Lincoln knew that slavery was vital to the economy of the south and that if he wished to preserve the union, he would need to allow it⁽⁹⁾.

“My paramount objective is to save the Union, and it is not either to save or destroy slavery. If I could save the Union without freeing any slave, I would do it.”

The American Civil War was not originally about slavery, it was prompted by banking and economics. Trade disputes had gone on between the north and south for decades and were exacerbated by their mutual trade partners in Europe. Two decades before the war, the US had gotten rid of its Central Bank (The 2nd Bank of The United States) but the central bankers weren't happy and looked to heighten the conflict so they could be seen as the solution to the problem. The Central Bankers of America had coincided interests with their European banking counterparts. Otto Von Bismarck, the Minister President of Prussia notoriously stated⁽¹⁰⁾,

“The division of the United States into federations of equal force was decided long before the Civil War by the high financial powers of Europe. These bankers were afraid that the United States, if they remained in one block and as one nation, would attain economic and financial independence, which would upset their financial domination over the world. The voice of the Rothschilds prevailed... Therefore, they sent their

emissaries into the field to exploit the question of slavery and to open an abyss between the two sections of the Union.”

We have seen that financial systems have a direct impact on the propagation of war. Now let's look at how Bitcoin can fix this. It's an important detail to note that all wealth throughout history has ultimately been protected by arms and the threat of force. At the end of every government policy is the threat of force. In an extreme example to illustrate this, let's look at tickets for something relatively benign like speeding. If you get a traffic ticket for \$200 and don't pay it, your fine increases to \$400. If you don't pay that, you get a court summons. If you don't show up to court, a warrant can be made for your arrest. If the police come to arrest you and you resist, they will use force to detain you.

This is true for government policy on an individual citizen level and is also true on a larger geopolitical level. So, it makes perfect sense that whichever nation has the greatest resources and biggest guns can control the wealth of other nations. If someone else had something, you could shoot them and take it. This is one of the limitations of physical commodities and centralized financial systems. Additionally, if you have massive resources and want to be more cunning than just shooting someone, you can use your tremendous wealth and influence to manipulate your enemy's centralized system because these systems are only as good as the people running them. If those people can be corrupted or confused, then a powerful group can exert control over it.

Bitcoin is a store of wealth that is not secured by might. Rather, it is secured by computational power and reinforced with cryptography. This means there is nothing physical for someone to take. There is something in crypto known as a “\$5 wrench attack”. This is a tongue in cheek hypothetical thought experiment used by cryptographers to contemplate security measures. It's a way of saying that if you wish to rob someone's crypto, you just buy a wrench and then use it to threaten them to give it to you. If that person hasn't taken proper security measures (security measures that have multiple layers), then they have an

ultimatum. They can give over their Bitcoin or choose to be assaulted or killed.

This would be no different than the physical confiscation of resources that happens in war. Thankfully, bitcoin can be stored in a manner that means confiscation by might is impractical. In the event of a \$5 wrench attack, if the assailant kills the bitcoin holder they will forever lose access to the funds. Thieves, by definition, want to rob, not kill. Some thieves may kill if they can ultimately get what they came for, but if killing the holder ensures that the robbery fails, then it's a natural fail safe.

If you imagine a \$5 wrench attack over physical money, then once the assailant kills the holder, they can just look for the cache until they find it. Why would an attacker go through the trouble of violence and the potential physical or legal repercussions of killing someone when they cannot even guarantee they will eventually get it? Similarly, this means that it wouldn't make sense to wage an entire war to take the wealth of a sovereign country that has their value stored on the Bitcoin Blockchain. A country would incur mass casualties and potentially still ultimately fail to obtain what their conquest was for.

Furthermore, it is of interest to note that The Federal Reserve and many of the other central banks of the world were founded in the late 19th and early 20th centuries. The fact that the 20th century was the bloodiest century in history might not be a coincidence. In fact, The Federal Reserve was founded about six months before the start of World War I. This topic requires an entire book in and of itself. Nonetheless, those that study history will recognize a relationship between finance, industry, banking, and the waging of war.

Central banks extend wars. They turn limited war into total war. Conflicts used to end when a country ran out of financial resources but, by having no restrictions on the printing of currency, central banks enable countries to fight beyond their resources and therefore extend the bloodshed and catastrophe.

If Bitcoin is about becoming one's own bank, then as more individuals become sovereign holders of their own wealth, they are no longer unintentionally voting with their dollars to give power to central banks and those that stand to benefit from war as an industry. Central

banks and governments have been able to fuel wars by jockeying for position to establish financial dominance. A sound money system based on strict rules removes the ability to game the system and jockey for supremacy over it.

Central banks, governments, and financial institutions will be able to interact with the Bitcoin Blockchain just like the rest of us, but they will be unable to exert influence over its rules. These entities have always been able to exert their influence by the intimidation or corruption of people. With Bitcoin, they are no longer dealing with people, they are dealing with an incorruptible programmatic set of rules. Taking away power from central banks by supplementing or replacing them with Bitcoin is like removing the kindling from the fire of war.

A World of Streaming Value and Micro Payments

When the internet was invented, its only capability was to send text-based information. It would have been difficult to imagine that someday that same technology would make summoning a ride from your cell phone a reality. Similarly, streaming TV shows on your tablet in the middle of the wilderness would not have been the logical conclusion of early internet adopters dreaming about future implementations of the technology. While we may be able to make some assumptions about what the future of blockchain technology will look like, it is unlikely that we can come even remotely close to envisioning many of the future implementations of it.

We can have a pretty good understanding of what the next several years will look like because there are already teams working on these projects. Greater efficiency in the transfer of value will enable us to ask fundamental questions about our existing systems - even ones we may not have originally thought to question, such as the practice of weekly or biweekly payroll. Why is it that our employers only pay us every two weeks? This isn't because they are trying to hoard our money away from us, it is because there are costs associated with tax reporting and filing and the transferring of currency from their account to ours. Wouldn't it be nice to get paid right at the end of your shift? With Bitcoin, the Lightning Network, and the use of smart contracts,

employers could offer daily payroll as a way to incentivize employees. Bitcoin would be the mode of transfer, the Lightning Network would make it fast and cheap (basically free), and smart contracts could ensure that appropriate taxes are withheld for both the employee and the employer.

The concept of streaming payments is one of the “big ideas” in the crypto space. Having a monthly membership to Netflix might be a good value proposition for the user that watches a lot of shows and movies on that particular service. But it makes them less likely to enjoy other services like Hulu. While some users will pay for multiple services, others will not. And even for those that do, the value proposition declines with each additional monthly subscription they pay for. They are paying for double the amount of content but do not magically have double the amount of free time to consume it. This means that they may be prohibited from watching some of their favorite shows if those shows are on a service for which they do not have a subscription.

The concept of streaming payments provides another viable option outside of the traditional membership model. Instead of requiring a monthly fixed payment, Netflix could allow users to stream payment only while they are watching a show. This means there can be more migration between users of various platforms. While this might not be enticing for an industry leader like Netflix initially (because they want users to *only* use *their* platform), it will be a massive value proposition to other streaming services. So essentially, if Netflix’s smaller competitors adopted the streaming payment model, Netflix wouldn’t be competing individually against Hulu, Vudu, Prime and others, but they would instead be competing against all those other services *collectively*. And Netflix would then be at a disadvantage and market forces would encourage them to adopt streaming payments. In the end it would be the users that benefit - as is typically the result when market forces are allowed to act in an organic way.

One might ask the question, “Why haven’t streaming payments been tried before?” It’s the same reason that even when iTunes started years ago that nothing was priced below 99 cents. Credit card processors charge fees that are simply too high for most businesses to profitably process payments for items less than 99 cents. It’s a simple but concrete

fact that means with the legacy payment processing system, streaming payments is an impossibility that is limited by their burdensome infrastructure. Second layer solutions like the Bitcoin Lightning Network (LN) have the capability to process transactions that are far less than the value of a penny. LN does this instantly and at virtually no cost.

From payroll to movies - these are just a few of the ways in which faster, cheaper, and more efficient payments can change entire industries. There are entirely new business models being dreamed up as you read this. The world is changing quickly, and blockchain is at the center of this transformation.

The Unbloody Revolution

When you begin to discuss the merits of Bitcoin and cryptocurrency as a whole, the conversation inevitably turns to, “But won’t the government just shut it down?” As you know by this point in your reading, that is no easy feat. It is practically impossible. The insinuation is that if Bitcoin is truly here to upend the establishment, then won’t the establishment just push back? Afterall, there’s a reason that the words “revolution” and “war” so often go together, right?

While I think Bitcoin will be one of the most profound revolutions in history, it may be unique in that it can be one of history’s only unbloody revolutions. Old, corrupt systems will hate aspects of the new, incorruptible system, but because Bitcoin represents a truly free market, there are still incentives for everyone. Those that already have wealth will not be banned from the network. They cannot be banned even if we wanted them to be.

In the same way that a free market benefits the poor and middle classes as well as the ultra-wealthy, it will provide freedom for those with wealth and power to benefit from the system as well. Sure, they will have to change their modus operandi. They will need to innovate and find ways to provide value to others and not just for themselves or they will risk becoming irrelevant. Governments don’t have to hate Bitcoin. In fact, I would argue that most governments love Bitcoin. Certain politicians may not, but that cannot be considered representative of governments as a whole. You might ask, “Why would governments love

it?” The industry is booming. Good, high-paying jobs are being created. Tax revenues are being generated. Those that adopt it will get an ego boost as being “forward thinking”.

Governments are already adopting Bitcoin en masse. When China banned Bitcoin mining, miners flooded to the US and other countries that had open arms. Cities like Miami, New York, and Austin are jockeying to be known as *the* Bitcoin city. El Salvador has adopted bitcoin as a national currency, and there are likely more countries moving in this direction soon. Hedge funds are investing in the space. Banks can now legally hold crypto in the US. There will be legacy players like Visa or Western Union that will be losers in this revolution, but such is true for any leap forward in technology - some entities will thrive, and some will be made obsolete.

Money affects almost every aspect of our lives. So, it makes sense that upending a system that controls our money would be a pretty nasty conflict. I have made the case elsewhere in this book that Bitcoin will be resilient in the event that the old guard puts up a fight. While there will certainly be some resistance, this does not mean all-out war. I believe many of the old guard got to where they are by being smart (regardless of whether they are moral or not) and I think they are already seeing the writing on the wall. They could choose to fight, but their intelligence may compel them to not resist the powerful current of innovation. When we look at incentives, I believe that a fair system is something that has the potential to align interests enough so that what may be history’s greatest revolution may be one of history’s only unbloody revolutions.

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government. We can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop"

- Friedrich Hayek,
Economist, 1984

The late Friedrich Hayek said it well. It's almost as though he predicted Bitcoin back in 1984. Perhaps we will have good money again. Not by force, but simply by adoption and people finding out it's a better system. The world's first unbloody revolution.

Chapter Six: *Breakdown of Crypto Asset Classes*

“On the dimension of technology, the conflict has two poles: AI and crypto... AI could theoretically make it possible to centrally control an entire economy. It is no coincidence that AI is the favorite technology of the Communist Party of China. Strong cryptography, at the other pole, holds out the prospect of a decentralized and individualized world. If AI is (Marxist), crypto is libertarian.”

- Peter Thiel
Preface of The Sovereign Individual, 2020 Edition

I have a particular passion for Bitcoin because what makes it unique from other crypto assets is that it fits the bill so perfectly as sound money. There are currently over 9,300 crypto assets listed on Coinmarketcap.com. Many more are unlisted. Since its inception, Bitcoin has had unchallenged market dominance. You may have heard of the term “Altcoin” before. The term altcoin applies to every other crypto asset besides Bitcoin - it’s essentially the market’s way of paying homage and recognizing that Bitcoin is the original and dominant asset.

Bitcoin is the most secure and decentralized crypto asset in the world, which makes it so inviting as the rails for a democratized worldwide payment system. While some aspects of this book apply to other protocols like Ethereum, please do not mistake everything I write in this book to represent all crypto assets. Having said that, I’m a big

believer in several of the other decentralized protocols that are emerging. They have real potential to bring decentralization to other aspects of life, which I think is sorely needed.

While the decentralized revolution will bring equality and fairness to many areas of our lives going forward, I believe the four biggest critical elements decentralization will positively impact for humanity will be in the areas of money, education, voting, and scientific research. Protection from central control and censorship in these areas will be a gigantic leap forward for humankind. In this section we will briefly breakdown some of the various crypto asset classes that currently exist. Hopefully this will give you a framework for better understanding the industry as a whole.

Money/Currency/Payment

Contrary to popular belief, not all crypto assets are attempting to be crypto *currencies* - a type of digital money. Bitcoin is obviously the leading candidate in the money, store of value, and payment arena. But there are other notable crypto currencies like XRP that focus specifically on international payment remittance.

These types of crypto currencies are typically defined by the limited supply of coins and/or predictable inflation rate of new incoming supply. It is very important to note that many crypto assets do not have a limited supply. In the investment section later on we will discuss “cheap coins” versus “expensive coins”. It is very important to recognize the major difference between coins with limited supplies versus those with unlimited supplies and inflation rates that are far worse than anything The Fed has ever done.

It is also important to note that not all crypto currencies that aim to act as money are decentralized or have the type of fairness and equality built into them that Bitcoin does. Stablecoins (coins that are tied to a fiat currency - ie: \$1USDT [Tether] = \$1USD) are highly centralized entities that have built more efficient versions of fiat currencies. So, while they work quite well at transmitting value, they hold almost none of the important monetary qualities of Bitcoin.

Notable crypto currencies that aim to operate as money and payments include but are not limited to: Bitcoin (BTC), XRP (XRP), Monero (XMR), stablecoins like Tether (USDT), DAI (DAI), and Hedera Hashgraph (HBAR).

dApps (Decentralized Applications)

If cryptocurrencies are like money or gold, then dApp crypto assets would be like oil - they provide the fuel for a wide assortment of decentralized programs. They harness the power of smart contracts to perform transactions without a middleman. So instead of the company Uber charging a fee for matching riders and drivers, a smart contract can perform that same function.

Remember, the essence of truly decentralized crypto assets is the removal of third parties and middlemen. dApp platforms like Ethereum will be a critical component of decentralized programs going forward. While holding Bitcoin is a bet on a new financial system, holding Ethereum or other dApp protocol coins is a bet on disruption in almost every other industry. You can think of it this simply: if it has a middleman, then it can potentially be disrupted by a dApp.

There is some confusion in the relationship between a dApp platform coin and a dApp token that operates on that platform. Coins and tokens are technically two different things. We typically call base protocol digital assets like Bitcoin or Ethereum a coin and we refer to dApp assets as tokens. In our example of the decentralized Uber - drivers and riders would exchange dUBER *tokens* for payment while using that dApp, but the small network fee (known as a gas fee) required to process that transaction on the Ethereum blockchain would be paid in ETH *coins*.

A simple way to think of dApp protocols is that they are like the base layer for the rest of the decentralized economy. The base protocol that makes the internet function is TCP/IP and then there are companies that have built their apps like Amazon on top of that protocol. This is the same kind of relationship Ethereum has with the dApps built on top of it.

Notable dApp protocols: Ethereum (ETH), Cardano (ADA), Solana (SOL), Polkadot (DOT) and Tron (TRX).

DeFi (Decentralized Finance)

DeFi is quite possibly one of the most exciting areas within the crypto industry. DeFi has the Bitcoin ethos of removing the necessity for powerful entities to control our access to capital. Access to capital is one of the most important elements in a capitalist economy - I mean, it's in the name, afterall. Our current credit-score based system for access to capital benefits some while keeping others out. It's a very narrow metric that does not necessarily accurately reflect an individual's financial health.

I started my first business when I was 22 years old. Because I had such a short credit history (anything under seven years weighs heavily against one's credit score) I was unable to access financing with good terms. A credit system that pigeonholes young people toward a path of college rather than building a business seems a bit skewed. This is one of the elements I refer to when I talk about how our financial systems are weighted against some while they favor others. Elon Musk sums this concept up quite well:

“The fact that an 18-year-old can’t take out a \$10,000 business loan, but can take out a \$100,000 student loan tells you everything you need to know.”

Without getting too much off into the weeds of the problems with student loans, let's look at how this system has been tailored to benefit large institutions while hurting and massively indebting young people. Some people vote for policies that make student loans easier for more young people to access because they think this will help them. But what are the economic effects? More potential students mean universities can raise their prices (because they only have so many spots after all - supply and demand forces prices up). These higher tuition prices force students to take on *even more* debt, which only further perpetuates this cycle.

To start my business at 22 years old I was able to get access to capital, but to say the terms were bad is an understatement. My wife and I had to get a variety of small loans and credit cards to finance our startup. The loans ranged from 15-19% interest and the credit cards had very *credit cardy* interest rates of 23-28%.

Within their first year, 21.5 percent of businesses fail, 30 percent in the second year, 50 percent in the fifth year and 70 percent by the tenth year⁽²⁶⁾. It is very difficult to build a successful business as it is, but access to only expensive capital stacks the deck even further against new businesses, especially young entrepreneurs, and other disadvantaged groups.

By the grace of God my business has survived and thrived past this ten-year milestone. But sadly, when we opened our first store, four other stores opened in our shopping center within six months and none of them are still in business. Each one was crushed by their unfavorable capital terms. And each of these business owners signed personal guarantees for their debt so even after their businesses closed, the fallout followed them for years beyond that.

DeFi provides an opportunity for individuals and businesses to get access to capital based upon their assets rather than their credit score. DeFi is quite simple, one person acts as the lender and provides capital while the other puts up collateral. Because these debts are collateralized, the two individuals do not even need to know one another's names, let alone a credit score.

A smart contract provides the only connection necessary in this relationship. If the debt goes unpaid, the smart contract liquidates (sells) some or all the collateral to pay the debt. This is a very safe investment for the lender because they are essentially guaranteed to get paid either through the regular payments or through liquidation of the collateral.

There is also an element of limiting risk for the borrower as well. With our current finance system based on credit scores and personal guarantees, when a borrower defaults on their loan, it adversely affects their credit score and the personal guarantee means that even once their business has failed (and they are presumably in a poor financial situation), they will still need to make payments on their debt. This can

be crippling and make the damage from the business failure go far beyond just a broken dream.

When a borrower uses collateral to access capital via DeFi, they know what their maximum potential loss can be: their collateral. If they default on their debt, their collateral will be liquidated, and their debt will be satisfied. In most cases only a portion of the collateral will be sold, meaning they will actually get some back. They may still be brokenhearted from the failure of their business, and they may be back to a financial square one, but this is far better than being in a financial hole.

The beautiful part about DeFi is that regular individuals can now participate in both sides of finance. Historically, only large institutions could be lenders. With DeFi, you can be a lender with any amount of money, and you can borrow virtually any amount. You can act like one of the big boys (banks) no matter what your budget is. Because these DeFi lenders are providing directly to those who want to access capital and therefore there is no middleman, they get the full amount of interest on the investment contract. Banks have become the wealthiest institutions on earth for two reasons: because they can create currency, and because they were essentially the only game in town for lending. They built financial empires doing this because it is wildly profitable. Bitcoin takes care of the problem of currency printing and DeFi empowers individuals to harness the same power that made the banks such wealthy entities.

Notable DeFi protocols: AAVE (AAVE), Maker (MKR), Magic Internet Money (MIM), Spell Token (SPELL), and Compound (COMP).

Oracles

Smart contracts will be the base protocol for pretty much everything in the future, but smart contracts can't be truly decentralized or trustless unless the information that goes into the contract is also decentralized. This is where oracles come in. They are the decentralized tool that collects the data that goes into a smart contract.

For example, if you and I bet on the Super Bowl via smart contract, who gets to tell the smart contract after the game is over who won? Whoever gets to input that information could totally corrupt it. So,

oracles are an algorithmic way to fetch the data about who won the game from a variety of sports betting and news sites. If the oracle gets a consensus that says the Rams won, then that's what would get put into the smart contract to execute it so the one who bet on the Rams gets fairly paid.

I believe oracles are one of the most under-appreciated asset types of digital assets. Smart contracts will be at the heart of most aspects of our lives in the future in the same way the internet is today and an absolutely critical piece of the smart contract infrastructure is oracle data.

Notable Oracle protocols: ChainLink (LINK), Band Protocol (BAND), Tellor (TRB), and XYO Network (XYO)

DeX's (Decentralized Exchanges)

DeXs play an interesting role in the crypto industry. They serve as a great example of how using smart contracts can cut out middlemen. A DeX is an exchange where you can trade one asset for another but rather than a company providing this service, it is performed algorithmically by a smart contract.

DeXs are also considered part of DeFi. This is because for markets to have liquidity (meaning that if you want to buy a token, there must be someone on the other end of that trade wanting to sell you that token) there must be liquidity-providers (LP's). All that means is that you can get paid as an investor by lending your cryptos to the DeX so it has an inventory of assets users can buy and sell.

DeXs are not favored by governments and other establishment players because they are unable to exert control over them (governments do not like industries they cannot regulate), but they do provide an excellent free market tool that enables assets to be bought and sold in a fair way. DeXs are a place to find more exotic crypto assets than on your traditional centralized exchanges like Coinbase or Binance.

Notable DeX protocols: Uniswap (UNI), PancakeSwap (CAKE), Sushi (SUSHI), Bancor (BNT) and 1inch (1INCH), Orca (ORCA) and Sundae Swap (SUNDAE).

Layer 2 Scaling Protocols

Layer 2's are essentially supplementary protocols that enable better functionality of the base layer protocol. In other words, a layer 2 is like a secondary network that assists the primary one by processing transactions and reducing the workload. For example, Bitcoin is very decentralized and secure, but those features come at a cost - they make Bitcoin relatively slow. Being decentralized and secure is a perfect foundation for a financial system, but in order to achieve adoption as a payments network it requires speed and cheap fees. For Bitcoin, this is where the Lightning Network comes in. This protocol transmits BTC between parties in seconds and essentially compiles thousands of transactions into batches and only settles them on the blockchain periodically. Users get funds instantaneously and the Lightning Network significantly reduces *traffic* on the main blockchain. Polygon is a layer two solution that essentially performs this same function, but for the Ethereum blockchain instead.

Other layer two solutions like Cosmos are attempting to make the various blockchains more interoperable. Currently, blockchains are considered "siloes" meaning they are protocols that do not communicate with one another. This is similar to the precursor of the internet. Before the World Wide Web, various universities had their own *intranets* where students and faculty could communicate with others at that specific university. When TCP/IP came along, it provided a bridge between these various intranets and connected them into the *internet*. In a nutshell, this is what layer two solutions like Cosmos aim to do for the various blockchains - connect them all into a network of networks and making them far more scalable.

Notable layer 2 protocols: Cosmos (ATOM), Polygon (MATIC), Bitcoin Lightning (there is no Bitcoin Lightning coin, this layer has no coins of its own), and Arbitrum (ARB)

NFT's (Non-Fungible Tokens)

You may remember from earlier that one of the necessary attributes of money is fungibility. This just means that one gold coin is the exact same value as another gold coin. Simply defined: fungibility just means something is interchangeable. That's a great quality for money and currency, but it's a terrible quality for something like art. The aim of the artist is to create something that is one of a kind. This is a major reason why NFTs have found tremendous adoption in a very short period of time within the artistic and content creation community.

An NFT is a limited supply token (it can be one of one or another limited number like one of one hundred) that represents ownership of a digital item. For example, anyone can go online and copy and paste an image of the Mona Lisa, but that does not mean you own the classic painting. What you have is simply a digital copy of it. Companies like Twitter have already integrated NFTs into their platforms by allowing users to exhibit their NFT as their profile picture and this comes with validation that the account is the actual owner of that content.

Yes, there is a vanity component to this, but when we sit back and consider the intellectual property side of NFTs paired with the programmability of smart contracts, we could be looking at revolutionizing an entire industry. Think about it like this, if an artist sells a painting for \$100, that \$100 is the only revenue the artist will ever get from that painting. Say that artist becomes famous, and this painting becomes incredibly valuable over time. The painting may sell multiple times to different collectors for millions of dollars, but the artist would see none of that money. If they were to create an NFT, they could program a perpetual royalty into their artwork. That means they would receive, for example, a 10 percent royalty every time the artwork is sold in the future. This means entirely new revenue streams for content creators and owners of intellectual property.

Right now, NFTs seem to be in their juvenile phase, but as they reach maturity, the implications of this tech are massive. If those already adopting it are any indication, then NFTs are undeniably here to stay as the NBA, NFL, UFC, other worldwide sports franchises, record labels,

art auction houses, and even the likes of Disney have jumped into the NFT space.

The integration of crypto wallets to store NFTs on various devices including smart TVs is already happening. Samsung recently announced that the next generation of their Frame TV will have NFT capabilities as the Frame TV is a popular TV for displaying artwork while not in use.

If we want to dream further about the pairing of emerging technologies, there are some interesting implications in a synergy between NFTs and 3D printing, which gets better every year. I think there may be a point in the not too distant future where online shopping or shopping in the Metaverse will allow you to pick out an item like a new pair of shoes, those shoes will have a specific NFT validating ownership rights to be able to print that pair of shoes and then you will be able to 3D print those shoes in your living room from your own 3D printer. This sounds far-fetched by today's limited versions of these technologies, but if we extrapolate them out, I believe this is an entirely real possibility.

Notable NFT protocols: Theta Token (THETA), Decentraland (MANA), Chiliz (CHZ), Flow (FLOW), and Ethereum Name Service (ENS)

Metaverse & Gaming

On October 28th, 2021, Facebook rebranded to Meta and sent shockwaves around the world. News channels had expert after expert on to explain what the implications of this were. Many people had never heard of the metaverse before this and then suddenly it was part of our day-to-day lexicon. In a nutshell, the Metaverse is a digital world. Individuals can play games, gamble, buy NFTs, or do a variety of other things as if they have a second life. The Metaverse became popularized in geeky tech circles in 1992 when the sci-fi book Snow Crash by Neal Stephenson was published.

Crypto gaming falls within the realm of the Metaverse. While there are certainly crypto gaming platforms that exist outside of digital

worlds, it seems as though there is a growing synergy between these two elements. In a simplified sense, crypto gaming is the evolution of games in order to “up the stakes”. Gen Xers that played Super Mario Bros when they were young remember running around on a 2D screen collecting coins. What was the purpose of those coins? I don’t know. But crypto gaming makes those coins worth something. Talk about a paradigm shift - there are already, today, people living in developing nations that are playing crypto games and earning a living by doing so.

Digital worlds and crypto gaming may seem like they have no place in a serious discussion, and even as someone that is thoroughly entrenched in the crypto space, I even have a hard time imagining how the Metaverse has utility in humanity's future. But it's important to understand the generational differences between older individuals (Baby Boomers and Gen X) that are considered digital immigrants and younger generations (Millenials and Zoomers) that are digital natives.

This is just a fancy way of saying that if you’re older than 40, you grew up before the internet was mainstream and certainly before the mobile internet was. I’m an older millennial and this is still something I have a difficult time seeing the value in. Younger generations are digital natives in that their school, social connections, and entertainment are largely online. For doubters of the Metaverse and the importance of crypto gaming, we should at least have the humility to see that digital worlds are not all that abstract to young people.

Notable Metaverse & Gaming protocols: Decentraland (MANA), Axie Infinity (AXS), Enjin Coin (ENJ), Bloktopia (BLOK), and The Sandbox (SAND).

DAOs (Decentralized Autonomous Organizations)

If dApps are the foundation that the decentralized future is built upon, then DAOs are the governance model. Simply put: if you have a decentralized application, how do you ensure that it continues to run, make improvements, and serve the customers who want to use it? You need a decentralized group of individuals with a common interest to do that work. That’s what a DAO is - a group of people who probably do not

even know one another that perform the function of a corporation but without a central structure.

I believe DAOs will change the face of business and provide a pretty cool solution for regular people without massive sums of capital themselves to create organizations that provide needed services to others. DAOs are only in their infancy and are experiencing growing pains as these organizations navigate new business structures. But, like many of these technologies, we can attempt to look around corners to see what the future holds as we work through these hurdles.

Notable DAO protocols: Dash (DASH), AAVE (AAVE), Decred (DCR), Synthetix (SNX), Atheneum (AEM), and Uniswap (UNI).

Note: the mention of various crypto assets in this section is not an endorsement of them. If you are interested in a particular field within the crypto industry, this section should only serve as the very first step in a much more in-depth research process.

Now that you understand the basic tenets of Bitcoin, you can stop reading. But, like any good evangelist, you might want to be prepared with a deeper, more robust understanding of the entire context around Bitcoin. Earlier, we discussed sound money. In the same way that sound money is helpful for understanding how to better answer the “Why Bitcoin?” question, getting a broader understanding of the history of money and how our existing financial system functions will only make the case for the decentralized revolution even more compelling. When you talk to grandpa about Bitcoin, it may be a totally different conversation than if you’re talking to your significant other. The information going forward should enable you to answer questions that both may have. Or, you may just find the subject of Bitcoin fascinating and you desire to expand your knowledge from a 101 understanding to a higher level. The following chapters will be filled with helpful analogies and deeper concepts that are still digestible, even for those new to the subject.

Chapter Seven:

Problems With the Current Financial System

“It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning.”

- Henry Ford

We have been raised in a world where governments have assumed the right to control the currency. And because the public has such a baseline trust of the government to act in good faith on this issue, most people do not realize that this privilege was actually *given* to large banks and captains of industry. It has not always been this way. The government certainly has influence over economic matters through policy, but in the US, as in many other prominent nations, the government does not specifically run the currency.

All the major countries around the world and throughout recent history have converted to a central bank model. Since it is all we have ever known, we assume that it is the inherent duty and right of the government to decide who runs our monetary system. But that simply isn’t true. There is no law of nature that dictates this role of government or banks. Bitcoin represents the first worldwide monetary network where

anyone can have access, regardless if they are rich or poor. Even a widely adopted money like gold was so precious and expensive, even in its smallest units, it couldn't be used by the poor. A gram of gold (too small to be a coin so it comes as flakes in a tiny bottle) is currently around \$60. Gold is not divisible enough to be accessible to all people. BTC, on the other hand, can be divided down to amounts far less than a penny, making it accessible to even the poorest individuals in the world.

Bitcoin represents an opportunity for humanity to have an alternative to transact value that is outside the scope of their sovereign government fiat currencies. To fully understand how massive these implications are, we must first better understand our current system.

Why Economics Matter

War, famine, sickness, malnutrition, crime, and a myriad of other social problems are the result of economic decisions. Decisions made at the societal level and the individual level factor into these outcomes.

Every decision an individual makes is economic. That might sound hyperbolic but it's not. When someone eats a meal, they are making an economic decision about what restaurant or grocery store they want to buy from. The skeptic of this point might say, "Aha! But what if I choose not to eat that meal at all?" That is also an economic decision. The restaurant you would have otherwise eaten at will be slightly negatively affected as they miss out on your money while you will economically benefit by saving that money.

Let's continue down this thought experiment on the individual level. One might say, "I didn't spend any money tonight because I didn't go out, I just stayed in and watched Netflix." That individual may not have performed a financial transaction that evening, but her decision was still economic. Her monthly Netflix subscription has a daily cost. Her views on whichever shows she watched gave feedback to Netflix and those ratings help Netflix determine whether a show is profitable for them or not. And again, her decision to stay in rather than go to Disneyland for the evening was an economic miss for the so-called Happiest Place on Earth.

By extension, all actions we take are political as well. Where one spends their money, even if in only a small way, tips the scales of power toward one side or the other. Each dollar spent is like casting a vote for that company, their ideologies, and their politics. In the same way that individuals cannot make any decision that is not economic, most certainly governments cannot either. While the economic decision of an individual might determine whether they are rich or poor, the actions of governments have implications for entire populations. Of all the actions the US Congress has ever made, no decision was more distinctly financial than its decision to empower a United States central bank - misleadingly called The Federal Reserve - to have a mandate to control its currency. There is a strange and mysterious relationship between the government and The Fed. The government spends and creates debt, and The Fed does what it can to make those problems go away by kicking the can down the road and keeping the gravy train flowing.

In a podcast by Robert Breedlove, a prominent economist and Bitcoin writer, he paraphrased a statement by the five term Chairman of The Federal Reserve Alan Greenspan, “A sound store of value must be made illegal or else fiat will not be competitive.” Breedlove’s response eloquently states how the practices of central banking caused the free market to create Bitcoin:

“This entire system we’ve built is a complex of unintended consequences (The Fed), and Bitcoin is an immune response from the collective economy.”

The American Founding Fathers expressed deep concerns about the power and influence that banks have over our democracy. Perhaps there is no more dangerous force than a convoluted and opaque partnership between the government and a banking cartel - something that appears to have been at the forefront of their minds:

“I sincerely believe that banking institutions are more dangerous to our liberties than standing armies. The

issuing power should be taken from the banks and restored to the people to whom it properly belongs.”

- Thomas Jefferson,
*3rd President of the
United States of America*

“History records that the money changers have used every form of abuse, intrigue, deceit, and violent means possible to maintain their control over governments by controlling money and its issuance.”

- James Madison,
*4th President of the
United States of America*

There is a well-known story in the Bible of the singular instance of Jesus exhibiting righteous anger. What was such an unjust and egregious offense that an otherwise humble man would throw over tables and ferociously call out the perpetrators in a place as holy as the temple of Jerusalem? Money changers ran a scam that took advantage of the innocent and unsuspecting. Jesus called out various sins in his ministry, but the one that prompted him to exhibit a righteous anger was a morally corrupt financial scheme.

During the time of Jesus, Jerusalem was under Roman rule. All forms of money at this time had the images of pagan rulers on them - except for one. The Jewish shekel was considered a holy currency because it did not violate the second commandment - *thou shalt have no idols*. For those coming to the temple to make their offering, they needed to pay the temple fee of a half-shekel and “pagan” currency was not accepted. Jews came from all over the world to visit the temple and give

an offering. This meant that vast amounts of money flowed into the temple. The money changers notoriously charged exorbitant fees, taking advantage of humble Jews simply wanting to perform a religious action. The scam was to exchange money at a vastly unfair rate, but temple-goers literally had no other option. The temple money changers had a virtual monopoly on God's forgiveness of sins and used that to extract wealth from the people.

Seeing this corruption prompted Jesus' only recorded display of righteous anger. Jesus didn't mince his words. He called these corrupt profiteers "A den of thieves." He could not allow the corruption to stand; the Bible says he threw over tables and fashioned a whip to drive the crooks away. This is perfectly in line with what was written about God's character over 700 years before Jesus was born.

"The LORD detests dishonest scales (for commerce), but accurate weights find favor with him."

- Proverbs 11:1

Regardless of whether you believe Jesus is God or whether Jesus was just a man, the fact of the matter is that the most influential person in history showed no sympathy for a corrupt financial system, and although he was typically quite calm, this type of injustice was deserving of a powerful expression of righteous wrath.

National Debt

"Some will rob you with a six-gun, And some with a fountain pen."

- Woody Guthrie,
Song: Pretty Boy Floyd

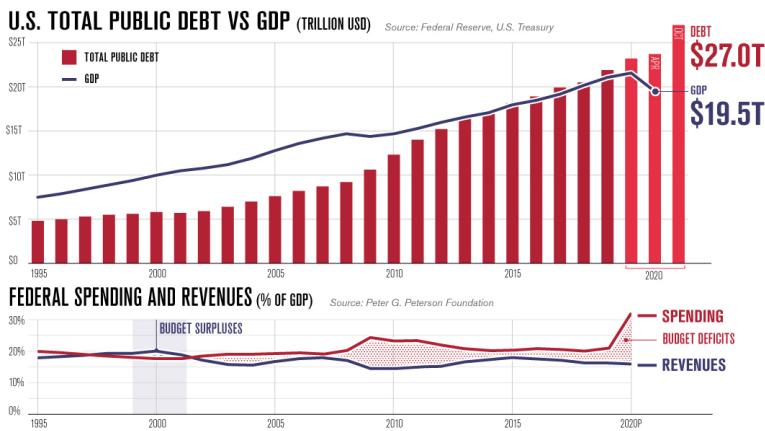
We learned a lot of things as a society from the 2008 financial crisis: don't buy a home with a variable rate mortgage, both Democrats and Republicans like to spend money, bankers that commit explicitly criminal acts not only get off scot-free, they still have the power to lobby politicians to pass legislation that gives the bankers money. In that time, a "massive" stimulus bill was \$700B. In a post 2020 world that seems like small fries. Nonetheless, it added astronomical amounts of debt to a country that already had a lot of debt. Instead of paying down this debt since the recovery, US debt has grown by almost 100 percent. It's now trillions of dollars higher than our country's entire economic output, commonly referred to as Gross Domestic Product (GDP).

The recession caused short term pain for some - mostly those in the lower and middle classes. While wealthy asset owners saw their wealth grow tremendously as the economy began to recover. In a free market system, recessions are to economies what small brush fires are for forests - they keep things in check so that things don't get too overgrown and susceptible to a catastrophic fire that burns everything down. Unfortunately, while our economy is described as Capitalist (which should mean Free Market), it is highly centrally planned and manipulated. The planners of our quasi-capitalist economy have not let these small brush fires happen - this is in part why we have seen the longest bull market in history since 2010 and even through Covid-19 that shut entire economies down to almost zero.

It makes very little sense that this once in a lifetime event (Covid-19) wouldn't even trigger a recession. It is unfathomable in a natural economy that absolute shutdowns of businesses wouldn't trigger a depression. It's because those centrally controlling the economy continue to juice the system with capital. This isn't only in the US either, systems around the world keep getting propped up by governments wanting to avoid short term pain. Afterall, what kind of politician will get reelected if he allows a recession? It's politically prudent to kick the can down the road while he's in office and let the next guy handle the chaos.

Where has this type of central control gotten us? A US national debt of \$29.87T. This is expected to grow to \$39T by 2030⁽¹⁷⁾. Let's break this down a little bit. In 2020, the US spent \$371B on interest

payments alone for the national debt⁽¹⁸⁾. This grew to \$562B in 2021⁽¹⁹⁾. Again, that's interest only, no principal. For reference, the US spent \$725B on the entire military in 2020⁽²⁰⁾ (more than the rest of the world combined). At our current pace, by 2030, our country's debt interest



payments will be greater than our entire military budget, taking over the number one spot as our country's highest expenditure. If you had a friend and you were helping him with his personal budget and it turned out that the minimum payments on his credit cards were greater than his mortgage payment, you would say something is most definitely wrong.

I literally had to continually update this number by substantial amounts as I wrote this book because the debt is growing so fast. If you want to go to the most depressing website ever, go to www.usdebtclock.org. It shows the US national debt in real time and it's a sight to behold. For some perspective, according to that site, \$29.87T in debt equates to over \$89,000 of debt per man, woman, and child, or more than \$238,000 per taxpayer. Look around at the people you know and ask yourself if that's a debt you think everyone you know could realistically pay off? No. Never. And that's the answer to this whole thing - we can't pay it off, and since we know that answer, then, like any good chess player, we need to start thinking a few steps ahead. Game Theory dictates that a knowledgeable chess player will base his moves off an analysis of his opponent's options. Once he makes a thorough analysis of his

opponent's possible moves, he reacts in the most advantageous way possible. Likewise, if we are looking to benefit from this transfer of wealth during this inflection point in monetary history, then we better know what the government's potential options are.

It's quite simple. The government has three options:

- A. Austerity
- B. Default
- C. Pay off the debt by devaluing the currency.

Let's briefly look at the viability of each of these options:

Austerity - In relation to fiscal policy, austerity simply means that the government would become stricter in terms of spending. To get out of debt, the government would need to do exactly what an individual would need to do: spend less money than they earn. If the government were to get out of debt by this means it would require massive cuts to entitlement programs like social security and other social safety nets. This would be very painful for many Americans. Politically, it would be wildly unpopular for an individual that attempted to push for it.

Even if politicians were able to get significant cuts to government spending done, it would likely cause a recession, or perhaps even a depression. The short-term effects would be incredibly painful (like an addict coming off a drug). The positive effects would take years to emerge. Politicians would have to convince citizens to continue with the pain even though they wouldn't see the benefits for years to come. Before healing could happen in the financial system and any meaningful amount of national debt paid off, the austerity politicians would surely have been voted out of office and replaced with those who would continue a looser policy.

For austerity measures to pass, we would need politicians acting counter to their very nature. No politician will push for something that people (in their ignorance of the subject) do not want and who will surely end their political hopes. The only remedy to this is to extend political terms (even as high as an eight or ten year term) so that long time horizon policies would have an opportunity to germinate and grow

before said politicians were up for re-election. This is also an unpopular remedy. Considering all of this, I think it's fair to put the prospect of this option happening at about zero percent.

Default - Governments, like individuals, have the option to not pay their debts. This is known as defaulting on a loan. Some might think that defaulting on our debt is a favorable option since big portions of the US debt is held by China, an economic adversary. The idea of snubbing an enemy does not bother many people. But it's important to realize that most of the national debt is actually owed to Americans - US Treasury Bond holders. While not paying China back might be palatable for some, the idea of defaulting on debt to ourselves is certainly less realistic. I have yet to see a single US bond-holder volunteer to forgive the debt that is owed to them by the US government. And why should they? They lent to the government in good faith and should be paid back in good faith.

The prospect of Americans voting to take money out of their own pockets is even less likely than austerity. So, we'll put this option at a zero percent likelihood of happening as well.

Pay off the debt by devaluing the currency -

If the first two options have a zero percent probability of happening then it looks like the only option is going to be #3. History indicates this as well. Here's a really important fact, in the history of fiat currencies and exorbitant national debts, 100 percent of the time governments go with option #3. Why is this the only option? Because no one really seems to mind it all that much while it's happening. They get the benefits of big government spending; easy access to capital because of low interest rates and they don't feel as though they are being taxed to pay for it (they are absolutely wrong about this, but it's hard to change how people feel).

One might ask, how does devaluing currency make it easy to pay the national debt? Let's do a bit of a thought experiment. Imagine a country with \$150 in circulation. The citizens have \$50, and the national debt is \$100. An economy of \$50 would have a terribly difficult time

paying down a debt of \$100. That would be a pretty substantial debt for that size economy. But, if the government decided to increase the money supply from \$150 to \$1,000 overnight, issuing all \$1,000 to the citizens, then it would only require a one-time 10 percent tax to pay off what had previously been an unpayable debt. The debt went from being 66 percent of the money supply to only 10% of the money supply. The debt itself didn't change, but its amount relative to the supply of currency changed. When debts are fixed and currencies are not, currencies will always be manipulated relative to the debt.

We will get more into the ins and outs of inflation later, but for now it's pertinent to see how the addition of currency into a system can affect a national debt. Most people are vaguely familiar with Germany's hyperinflation after WW1. Most people have heard the stories of how a wheelbarrow full of cash could buy a loaf of bread at the store. But what many people are not familiar with from that inflation is the sheer magnitude of it.

After WW1 and before the hyperinflation hit (hyperinflation is defined as a month over month inflation rate of 50 percent or greater), the Weimar Republic (Germany) had a national debt of about 60B Marks. This was a comparable amount to the US's current \$30T debt - considered an unpayable debt of war finance and reparations. Weimar Germany concluded that their only option was to turn on the money printers. After four years of hyperinflation, their currency spiraled so far out of control and became so worthless that their 60B Mark debt was now the equivalent value of 60¢! That's not hyperbole. There's no exaggeration. The currency became so devalued that the smallest bill in circulation was a one trillion Mark note! So how did Weimar Germany pay off their tremendous 60B Mark debt? They turned it into 60¢ and then it was no problem.

Not only was that financial crisis the cause of much pain and suffering for the people at that time, but the consequence of this poor fiscal policy was the rise of Adolph Hitler - further proving my earlier statement that economics matter.

If the US's debt problem does not seem problematic enough, look at the world's debt. According to Ray Dalio, in his book *Principles for Dealing with the Changing World Order*, as of 2021, there is \$16T in

worldwide debt that is at negative interest rates. This means that these debtors actually pay people to take on debt so they can have the freedom to print more currency (currency gets created when someone takes on debt). Imagine having a mortgage where the bank paid *you*. If that isn't a clear sign of an unhealthy system, I don't know what is.

If we understand the basic principle that fiat currencies are broken beyond repair and destined toward extreme inflation then regardless of what politicians and Federal Reserve officials say, we can tailor our financial planning appropriately. So instead of being tossed back and forth like a boat on the rough waters of uncertainty, as so many investors are, we can chart a clear course with a clear understanding.

It's a certainty that fiat currency devalues. They always have. They always will. Like the chess player who thinks steps ahead, the prudent investor should look for assets that are resistant to these effects. If fiat currencies are prone to inflation because they are not scarce, then a scarce asset is the solution. BTC was engineered with this very function in mind.

The Federal Reserve

“The financial system... has been turned over to... the Federal Reserve Board. That board administers the finance system by authority of... a purely profiteering group. The system is private, conducted for the sole purpose of obtaining the greatest possible profits from the use of other people’s money.”

- Charles A. Lindberg,
Congressman, 1923

Most people do not like to talk about the Federal Reserve because they do not understand what the Federal Reserve is. The default

belief by most Americans is understandably that The Fed is a branch of the government that deals with currency and fiscal policy. The Fed does deal with currency and fiscal policies, but it is not a government agency. It is a private business. It has shareholders. Shareholders make dividends from the profits it generates. It is given this power by Congress. This public/private collusion and the mysterious ownership structure is what creates so much confusion.

One of the things that makes The Fed a confusing organization to the public is that positions within it are appointed by the President of the United States. People also rationally assume that if some entity controls the currency of a country that it must be run by the government so that the people have some say over it. This, again, is an errant belief. The Fed is essentially a super bank that has the sole power to create currency. That's right, a private business is in charge of the currency for the US and most of the world. That's an amazing thought.

This is surely what Henry Ford was alluding to in the opening quote of this chapter, which bears repeating. *"It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning."*

Think of how much distrust the average American has for large corporations. Americans do not like that corporations have huge concentrations of power and money. Now think how much outrage there would be tomorrow morning if everyone collectively found out that the world's wealthiest and most powerful organization controls their currency and their banking system. Additionally, how much rage would there be at the fact that this entity's shareholders are kept hidden from the public? How much backlash would there be if people realized that this entity had never been audited? I think Henry Ford was right, there would be revolution in the streets if people only knew. But sadly, they don't.

The Federal Reserve was conceived in secrecy. One of the greatest true conspiracy theories of all time was the inception of The Fed. G. Edward Griffin's famous book, *The Creature from Jekyll Island*, details how it all happened. In a nutshell, we know about the secret origins of The Fed largely because those who created it later boasted about their conspiracy. Decades after the birth of The Fed it was deemed

a success, and this stroked the hubris of its founders. They confessed through bragging.

The condensed version is as follows. In November 1910 a group of six ultra-powerful elites traveled in a private train car and ferry to Jekyll Island, Georgia. On this trip was Nelson W. Aldrich (powerful US Senator, business partner of JP Morgan, and the father-in-law of John D. Rockefeller Jr.), Abraham Piatt Andrew (Assistant Secretary of the US Treasury), Frank A. Vanderlip (President of the National City Bank of New York, the most powerful bank at that time), Henry P. Davison (Senior Partner of The JP Morgan Company), Benjamin Strong (Head of JP Morgan Bankers Trust Company), and Paul M. Warburg (Partner in Kuhn Loeb & Co., Representative of the Rothschild banking dynasty, brother of Max Warburg, and head of Warburg banking consortium in Germany and The Netherlands). According to Griffin, these six individuals represented 1/6th of the entire wealth of the world at that time. So, to say these were powerful men, is an understatement.

The reason this meeting was so secretive was because the purpose was to design the plans for a new central bank in the US. At that time, Americans distrusted bankers because of widespread bank failures and nefarious banking practices. Americans were especially skeptical of central banks because the US had three of them in its history and none worked out. US citizens could see what was happening to Europe under their central banking regimes and they largely didn't like what they saw. But these powerful lords of finance knew that if they worked together instead of competing against each other, they would be able to amplify their influence and fatten their bottom lines.

One might say, "Oh that's nice that they want to work together." But the fact is, banks working together is anything but nice. It's collusion, and under US antitrust (anti-monopoly) laws, it was illegal. These brilliant individuals knew that if they planned meticulously enough, they could create a banking cartel that would leave their power unchallenged. What is a cartel? A cartel is a group of independent businesses that join together to coordinate the production, pricing, and marketing of their product or service. The purpose of a cartel is to reduce competition and increase profits. This forces the public to pay higher

prices for their goods or services than they would otherwise in a free market.

Doubling down on the point that The Fed is in fact a cartel, a year after the passage of The Federal Reserve Act, the grandmaster of this whole scheme, Senator Nelson Aldrich, stated this at the American Banks Association event:

“The organization proposed is not a bank but a cooperative union of all the banks of the country for definite purposes.”

And two years later at that same conference A. Barton Hepburn from Chase Bank said,

“...indeed, if it works out as the sponsors of the law hope, it will make all incorporated banks together, joint owners of a central dominating power.”

Do you think that if the American people realized their entire money and banking system was run by a cartel that they would be ok with that fact? I assume not. But most people think there's no possible way this can be true because “Who would have allowed it to happen in the first place?” That's a rational question, but it just goes to show the level of collusion that took place amongst these power brokers at the fateful Jekyll Island meeting. These men knew that the American public had no desire for a central bank. In fact, the American public would not be in favor of anything this group of elites put together because the public did not like monopolies and the ultra-wealthy.

This sentiment is echoed in a statement by Frank Vanderlip (one of these elites) two decades after the famed Jekyll Island meeting as he bragged to the Saturday Evening Post about their shenanigans:

“The servants and train crew (on their ride to Jekyll Island) may have known the identities of one or two of us. But they did

not know all. And it was the names of all printed together that would have made our mysterious journey significant in Washington, in Wall Street, and even in London. Discovery, we knew, simply must not happen. Or else our time and effort would be wasted. If it were to be exposed publicly that our particular group had gotten together and written a banking bill, that bill would have no chance whatsoever of passage by Congress.”

- February 9th, 1935

On that trip, these men agreed to a strategy to ensure that the bill would pass. Senator Aldrich would introduce the bill to the Senate, and he would declare it was an “anti-bank” bill to put in place regulations on banks that would protect the American people. The duty of the bankers from the Jekyll Island meeting would be to come out publicly against the bill. Their job was to convince the public that this bill would “crush them”. That it would be unfair to the banks.

This plan had about as much reverse psychology toward the American public as a parent uses when trying to get their child to eat veggies. But sadly, it worked. The Federal Reserve Act passed, giving the Fed the sole power to create and destroy currency and the power to set interest rates on debt. If you understand finance, these two powers essentially make you politically omnipotent, as money drives everything. The American public thought the passage of the bill would take power away from the banks, when in fact they were duped, and it gave banks vastly more power than they ever had before.

The Federal Reserve is the 4th central bank in the history of the United States. The first three failed because they each printed their currencies into severe inflation, depleting the value of their currencies by an average of 66 percent within only a few years. Each iteration of the US central banks modeled their structure after the European central banking models (largely because it was the European central banks helmed by the Rothschild family that exerted their vast influence over the creation of US central banks). This was a recipe for disaster. Popular

public opinion turned against the central banks in each generation, causing them to lose their bank charter. Then, once that generation passed away, the next naive generation welcomed a new central bank with open arms.

Why is a banking cartel so bad? Because a cartel or monopoly over banking is the most powerful kind of monopoly imaginable. The ability to print money at will and give it to those they see fit is a tremendous power. And this power comes at the expense of US citizens or anyone else that holds USD, as this currency is like a melting ice cube in the hands of the unsuspecting.

At the end of the day ask yourself, “Does it sit right with me that 12 unelected people sit in a room and decide the financial future of the entire world?”

Fractional Reserve Banking

For most people, the thing that sells them on the absurdity of our banking system is the practice of Fractional Reserve Banking. If you were to explain it to a ten-year-old, they would quickly tell you that that system could never sustain itself. Fractional Reserve Banking is the practice whereby banks take in deposits and are able to turn around and lend the majority of those funds back out. We all understand on some level that banks do this, that’s why they pay interest (although not much) on your savings account.

What most people do not realize is how much of their funds are actually being lent out. Since The Fed allowed the practice of Fractional Reserve Banking, banks typically had the ability to lend out up to 90 percent of funds they held. This meant that if you deposited \$100 into the bank, they could lend out \$90 to other people. Over time this policy became looser and the threshold was permitted to be 98 percent, meaning that only \$2 of your \$100 deposit had not been lent out. As you can imagine, this policy has become even looser and now banks are not universally required to maintain ANY threshold - meaning that they can lend out 100 percent of deposits. This means that if everyone went to the bank at the same time to get their money, only about two percent of

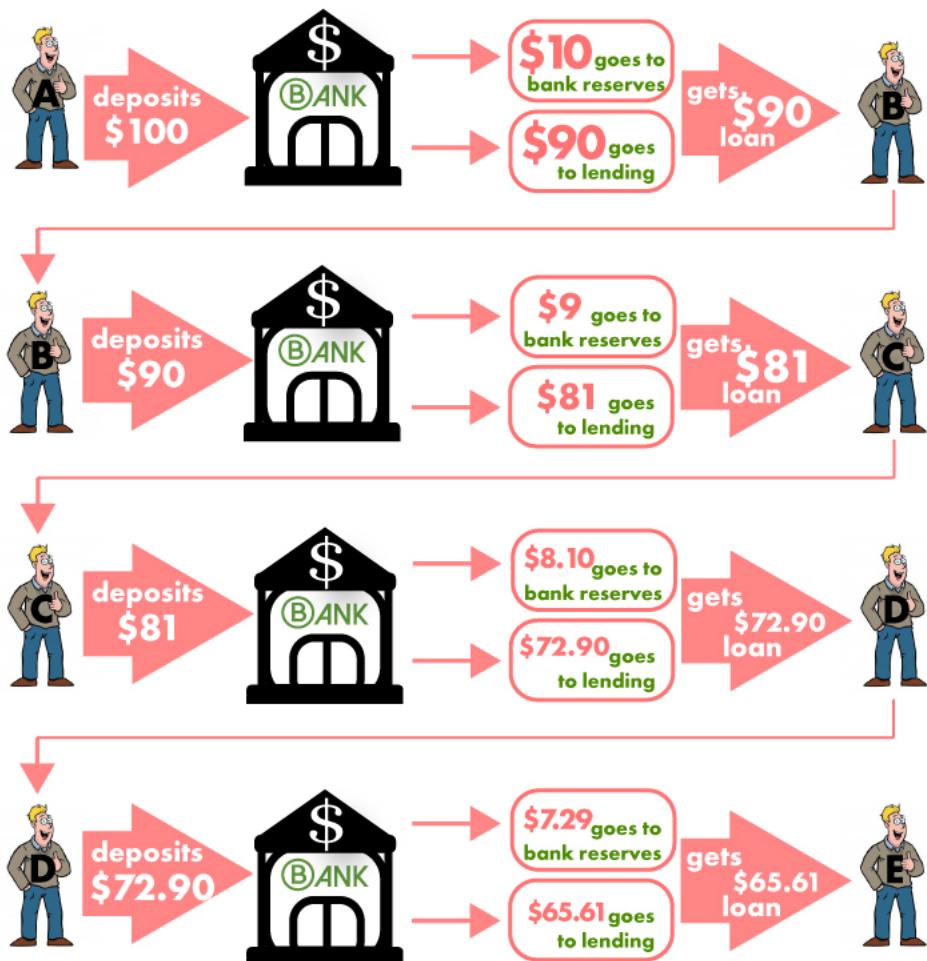
people would get their money. There wouldn't be any funds left available for the other 98 percent.

Bernie Madoff was sentenced to 150 years in prison and a \$170B restitution for running history's biggest Ponzi Scheme. A Ponzi Scheme is defined as an investment scheme where initial investors are not paid with profits from a legitimate business operation. Instead, they are paid with funds from new investors. It's such a dangerous scheme because it is unsustainable. You will not be able to find new investors forever. The gravy train will run out at some point.

This is true for Fractional Reserve Banking as well. Fractional Reserve Banking can turn \$100 of actual value into thousands of dollars in perceived value on paper. It's an utterly unsustainable system and those whose wealth is primarily in cash will be hurt the most when this house of cards comes tumbling down. Bitcoin offers a hard money alternative to cash that is outside of this flawed system. It's like a lifeboat for those that see the Titanic Banking System sinking.



Fractional Reserve Banking



\$100 of actual money deposited by Customer A turns into \$409.51 on paper after only 4 cycles. Keep in mind, these cycles can continue far beyond this, creating orders of magnitude more in “paper value” than the original \$100 deposit.

Other Banking Practices

“We have in this country one of the most corrupt institutions the world has ever known. I refer to the Federal Reserve Board... This evil institution has impoverished... the people of the United States... and has practically bankrupted our Government. It has done this through... the corrupt practices of the moneyed vultures who control it.”

- *Congressman Louis T. McFadden,*
1932

Banks are notorious for their “nickel and dime” tactics. Charging miscellaneous fees that the average consumer just accepts because they think it must just be standard practice. But ultimately, those types of practices are fair game because in a free market, patrons are free to take their business elsewhere. These practices become a problem when they are hidden, or they take advantage of their most at risk customers.

One of these practices was Wells Fargo’s infamous practice of signing their customers up for multiple unnecessary accounts. When I was starting my first business, I was involved in this scam being run by Wells Fargo. I have even received Class Action lawsuit checks to prove it. At that time, I wanted a business checking account, savings account, and a small credit line. I received all those things, but after a few months went by I noticed I was getting all sorts of other pieces of mail from Wells Fargo. In the end, they signed me up for three checking accounts and two credit cards with significant annual fees, none of which I asked for. It turned out that Wells Fargo corporate had been giving their bankers insanely difficult sales quotas for accounts and so their bankers took it upon themselves to sign customers up for accounts and services they didn’t even want.

Beyond these types of out and out scams, banks are well known for their massive annual revenue from overdraft fees. Yes, it is the fault of a customer if they overdraft from their account because it is their

responsibility to know their balance. But for years, banks were enabling this problem further by allowing their customers to charge their card multiple times after their account balance passed \$0. According to Forbes, in 2021 alone, banks collected over \$12.4B in revenue from overdraft fees⁽⁴⁵⁾. Are the wealthy the ones paying overdraft fees? Probably not. This is an unfortunate plight that disproportionately affects those who are already struggling with low balances.

“Student debt is a product that has been sold to us with such repetition and intensity that most people believe they can’t live without.”

– Unknown

Student loans and college degrees overwhelmingly do little to create wealthy individuals, and yet students have relatively easy access to funds for this purpose. But if a young person has a brilliant idea and wants to start a business to foster that idea, it is almost impossible for that person to access capital unless they are already wealthy. Banks have made common practice of lending to endeavors like college that create perpetual debt, and avoid lending to individuals for things like business and investments that can enrich that person.

How An Investment Crisis Happens in the Safest Investment Sector, Real Estate

“Tell me the difference between stupid and illegal and I’ll have my wife’s brother arrested.”

– *The Big Short*

There were many causes to the 2008 financial crisis and a lot of colluding parties that should share the blame. But since we are on the subject of the flaws of centralized systems of finance, it seems like an opportune time to discuss the role ratings agencies played.

Ratings agencies such as Standard and Poor's (S&P) and Moody's make their fortunes by evaluating investment products and then assigning them a rating. The rating provides consumers with an idea of how safe or risky an investment is. For example, housing bonds are investment products with hundreds or thousands of mortgages in them. A bond with only mortgages for people with credit scores above 720 would be deemed a safer investment than a bond full of mortgages for people with credit scores of only 600. A very safe bond would be AAA rated while a very unsafe bond would be rated a B.

So far, so good. This form of investment rating makes a lot of sense. The inherent flaw comes in when you look at the business model. Who pays the ratings agency to rate the bond? Alarmingly, it's the companies creating and selling the bonds that pay for these ratings. Imagine being the ratings agency where your customer is the very company creating the bond. One can easily see how wanting to please the client could create a conflict of interest in this process.

In the years leading up to the collapse of 2008 this conflict of interest reared its ugly head. Mortgage bonds full of toxic investments were being rated by the agencies as AAA. So regular everyday US citizens invested billions of dollars buying these for their retirement and other accounts thinking they were very safe assets. But in reality they were very bad.

Imagine a friend asks you to invest in his company. He shows you his financial statements and everything looks good, so you decide to invest. Six months later he goes out of business and tells you he lied on his financial statements. He misled you into thinking you were making a relatively safe investment, but he knew it wasn't safe at all. What he did would be illegal. It would be fraud. In the same way your friend would have committed a crime, the major US ratings agencies committed fraud on a global scale.

I have discussed throughout this book how incentives drive results. This is especially true for incentive structures obfuscated to the general public. Because of the way this system is constructed, incentives make it ripe for this type of collusion and fraud. This type of fraud can only happen in opaque systems. Open and transparent financial systems powered by Bitcoin create an environment where this type of fraud

cannot happen. Exposure to the light is one of the best disinfectants - this is true in virology, and it is true in finance.

Wealth Imbalance

As a Capitalist I am not a proponent of wealth equity - the idea that government should ensure that all citizens have exactly the same thing. I am a strong proponent of equality of opportunity, especially in financial systems. It is not the goal of all individuals to become rich. Some people value family time over late nights at the office. The financial goals of people vary significantly, so to try and create a system that forces everyone to have similar economic outcomes seems a bit foolish and frankly, unfair. This is the brilliance in providing an economic system where everyone has equal opportunity. Equal opportunity means that those who wish to become rich have a path to do so. Those that wish to live a simpler life and just provide for their basic needs can do so as well. Unfortunately, the current economic system we have in the US does not provide the same opportunities for everyone.

During COVID, \$6.5T in wealth went to the top one percent wealthiest people, while the rest of the 99 percent shared \$1.5T in wealth as you'll see below. This concentration of wealth can only be chalked up to the way in which our system is constructed. Those with wealth and power have vastly more access to free or cheap capital, which enables them to grow their wealth further. Those who are unbanked have limited or no access to capital. Proportionately, very little of the multi-trillion-dollar stimulus bills went to the poor and middle classes. Large entities received the bulk of these trillions of dollars either in the form of direct (free) money, or in the form of loans with almost zero percent interest and favorable repayment terms. Many of these loans could be forgiven if they were used for certain purposes deemed acceptable by the government. This was at a time when many of these same big box retailers were allowed to stay open throughout lockdowns while many other businesses were forced to shut down. While they were making all time high profits, they were getting money dumped on them from the skies.

Pharmaceutical companies were put in charge of making the world's most sought after product in history, which would be highly profitable even under normal circumstances, but these profits were made even greater because governments paid for all of the research and development of the Covid-19 vaccines. These companies got to have their costs paid for while also getting the privilege of having bureaucratic red tape (proper long term safety and efficacy studies) cut for them, they got billions of dollars in free advertising for their products and at the end of all that, governments and businesses mandated their products in many different sectors. This is the epitome of playing favorites.

In 2020, while many companies were literally put out of business by government lockdown mandates, other businesses were given massive privileges and money. But this type of easy capital access wasn't something that started with Covid. It has been occurring for decades. This imbalance of access to easy capital may not seem like a big deal to some, but when you understand something known as the Cantillon Effect it begins to become clearer. The Cantillon Effect is simple: when new capital enters the market it goes to the elite. These entities get to spend that capital at today's full value. As that capital flows down through the rest of the economy, others get to spend it as well, but they must spend it at the inflated value - meaning that their buying power with those same dollars is much less. It's the quintessential tactic of the powerful and privileged upper classes that allows them to maintain this wealth imbalance in a hidden way.

Allow me to illustrate this point. If you were a company in 2020 that received \$1M in stimulus from the federal government, you got to spend that money at 2020's value. The inflation rate in 2021 was seven percent and the inflation rate in 2022 was 8.5 percent. By the time that \$1M trickled down through the economy, the people who finally got to spend that money in 2021 only got \$930,000 of buying power (after seven percent inflation). Those that didn't touch that money until 2022 only got \$839,050 worth of buying power (one year of 8.5 percent inflation compounded on top of one year of seven percent inflation).

Bitcoin provides an economic framework where the creation of currency is taken out of the hands of a central authority and is distributed based solely on merit (mining), or by purchasing it at a fair market price.



The Cantillon Effect



Newly printed dollars go to the Billionaire. He gets to spend this money at today's full value because the economy has not recognized the new, larger amount of capital in the market.



Next, the capital flows to the Millionaire. The market still has not fully priced in this new volume of money because it hasn't touched many hands yet. Millionaire guy gets to spend it at its full value as well.



Next, the capital flows to Middle Class Guy and millions of other people like him. Since the capital is touching so many hands at this point, the market will start to price in inflation. Middle Class Guy will get less buying power than Millionaire and Billionaire.



By the time the capital flows to the millions and millions of people in the poorest classes, the market is totally aware of the additional capital in the system. Inflation will be fully priced in by the time these individuals get their hands on the capital and they will get the weakest buying power out of it.

The rules of this distribution are clear and fair. Everyone interacting with this system can audit this distribution at any time on the block explorer and they can verify the rate of new currency being issued. This fundamental change in structure means that Capitalism can thrive without the threat of corruption at its core - the unfair distribution of currency.

Deep Fakes and Censored Information

The internet is one of the most important inventions of all time, but it has one fundamental vulnerability in its current state: it's highly centralized. Additionally, the tech companies built on top of the internet are highly centralized as well. When you sit back and think about how much trust is put in these companies to keep our records on their servers, it can be a little unsettling.

United States Supreme court opinions, home deeds, medical research, scientific journals, hospital records, personal records, and government records are all stored on central servers. I'm not saying those who run these servers necessarily have bad motives but it's important to understand they wield tremendous power.

Let me ask a fundamental question: how do we know that American Colonists revolted against England and waged a war for their independence? How do we know that the colonists weren't always free? How do we know *any* of what we know? There's an entire field of study devoted to the question of "How do we know what we know?" It's called Epistemology. And the answer to these questions about the American Revolution is that we have physical source documents that provide us with these answers. Another way of saying this is that we have history books.

One of the major drawbacks as we transition from physical record keeping to digital records is that digital records can be altered quite easily and discretely. When the Nazis practiced book burning to silence dissenting opinion and erase history, they fought a tremendous uphill battle because they had to ensure that they burned every last copy. Even a single copy of a book with a dissenting opinion or historical record could undermine the entire Nazi propaganda engine.

Digital record-keeping is wildly efficient, but this efficiency also makes altering or deleting these records efficient as well. The word “Nookd” has made its way into the Urban Dictionary and serves as a foreboding example of alterations made to digital documents. Leo Tolstoy’s famous work *War and Peace* was apparently the unintended target of an algorithm gone awry. Individuals that read *War and Peace* on Barnes and Noble’s eReader the Nook got a slightly altered version of the story.

*“When the flame of the sulfur splinters **Nookd** by the tinder burned up, first blue and then red, Shcherbinin lit the tallow candle.”*

How does one Nook a splinter? You don’t, you *kindle* it. But unfortunately, Kindle is the name of Amazon’s eReader, the competitor of Barnes and Noble. This, in all likelihood, was a misfire and was not the direct intention of Barnes and Noble, but it perhaps indicates a more unscrupulous intent to censor mentions of their competitor and falsely replace it with the name of their own product on other media.

This should serve as an example of the efficiency of censorship across digital media. A single computer programmer can write up some relatively simple code to alter or even erase keywords, ideas, history or even people. When it comes to central servers, the stewards of that data essentially have omnipotence. Even in the event that the stewards of these records have the absolute best of intentions, data can always be unintentionally corrupted, lost, hacked or stolen.

A common practice in online journalism is something called “Ninja Editing”. Online publications have a highly nimble form of media. In the old days, a journalist that got something factually incorrect or expressed an opinion that was later proved incorrect would have to go through the process of a retraction. This meant that in a subsequent edition of their magazine or newspaper they would have to run a story essentially telling the public that they messed up and they would report the most up to date information.

With today's online publications, ethical journalists still abide by this process. But unfortunately, many do not. They simply go back and edit their story as though they got it right all along. The public is none the wiser and the writer gets to boast about their excellent editorial record.

Another growing segment of the digital world that is creating more potential problems than it solves, is Deep Fakes. A Deep Fake is a video that looks real but isn't. Computer graphics have gotten so good and so compelling that we can now take a video of someone and alter it to make it look as though they are saying or doing something they are not. One of the darker sides of this technology is a form of digital ransom.

With a quick online search, you can find dozens of stories of extortion using deep fakes. One such story was of a young, engaged woman. Somehow a group of Deep Fake criminals came across her online profile and used her pictures to overlay her likeness onto an adult actress in a pornographic film. The Deep Fake criminals sent her the video and told her that if she didn't pay them a ransom, they would send this video to her fiancé - insinuating that she had been unfaithful to him.

Imagine this same technology used in a nefarious way with political heads of state. Could a nuclear war be provoked by a Deep Fake video of the US President saying he was launching nuclear warheads toward China? How would the Chinese respond to that? To give this frightening thought more context, it's important to know that this technology is not inaccessible. Advanced college students can create compelling Deep Fake videos. This is a problem that needs a solution.

As someone who reads the Bible and believes that what it says is foundational truth, I find it very concerning that someday most of the records of the Bible will be digital. If billions of people depend on the Bible to be the greatest source of truth about our lives, then the altering of that book could be the most powerful weapon ever wielded against humanity.

In the Bible's physical form, we can trace its validity in scientifically accurate ways. For example, how would Jews and Christians of the 2000s know whether their Bible was the same as the Bible from ancient times? In 1947 archeologists found the earliest dated

manuscripts of the books of the Old Testament. These documents dated back as far as 300 BC and are known as The Dead Sea Scrolls.

From there a very simple analysis was run: does the Bible that we have today match the Bible from over 2,000 years ago? Yes. They match with over 95 percent accuracy (the differences are made up of punctuation and grammar). The Dead Sea Scrolls are considered one of the most important archeological finds ever because they prove the Bible was unaltered over a period of two millennia. The works of Shakespeare have been more altered over the last 500 years! It lends tremendous credibility to the Bible to be one of the oldest writings in existence and yet it has managed to be unaltered. Those who believe this is the manifested word of God have a very valid point when they allude to this fact about its reliability.

What a tragedy it would be for the Bible to last millennia only to come under attack because of the inherent vulnerabilities of central digital storage. Needless to say, whether we are looking for reliability in journalism, religious texts, or safe and accurate record keeping, these concerns are only growing as more and more of our lives are being stored digitally.

This begs the question, “What is the solution?” The answer is the blockchain. The transparency, immutability, and decentralized nature of blockchain provides the perfect remedy. To add a block of information to the blockchain, it must be openly broadcast to all other nodes on the network. Once consensus is reached, it can be added to the chain. But no matter how much consensus is reached, past blocks of information can never be altered.

In the example from above about the Bible, it is possible that someone could propose adding a new block of information with a new and different version of the Bible. Consensus could even be reached, and that new version could be added to the official record even though it is an inaccurate copy. BUT if there was ever a dispute as to which was the original version, we could always just go back to the blockchain and see which version was added first, thus making that one the more historically accurate version. Instead of needing to trust any central record keeping authority, we could just verify it for ourselves at any time. This is true for medical records, home deeds, personal information, scientific research

data, history, or any one of the critical pieces of information we depend on. This is also true for unique digital files like those that could be used for unethical or dangerous purposes like Deep Fakes. The future of digital recordings will integrate Non-Fungible Tokens (NFTs) into their file. This means that we will be able to cryptographically prove whether something is a genuine original or if it is simply a digital copy of another file.

The internet was a truly revolutionary technology, but it was incomplete. The blockchain is the capstone that makes the internet trustworthy, useful, and capable of handling our sensitive digital information. In other words, the blockchain completes the internet.

Bail-Ins: No Way, That Can't Be Real

Many people are unaware of what a Bail-In is. And people shouldn't know what it is because Bail-Ins shouldn't exist in a free society. In 2013 the government of Cyprus (a small Mediterranean island near Greece) closed its banks for a bank holiday without notice. The next day, citizens woke up to find that 10 percent of the funds from their savings accounts were wiped out overnight. There was no warning, and citizens had no recourse. The government told the citizens it was their civic duty to protect the island's banking system.

Some might call it civic duty while others call it theft.

Despite popular belief, bail-ins are already written into law in the United States. Bail ins became statutory in the US along with the Dodd-Frank Act in 2010. While bail-ins have not been used in the US, they are a tool in the toolbox of the government. Knowing that you could be called upon at any moment to perform a generous civic duty like giving 10 percent of your savings to The Fed overnight is one of the best sales pitches ever for Bitcoin. Having complete sovereignty over one's own money probably looks pretty good to the people of Cyprus.

An Immoral System

“Differing weights [on a scale, one for buying and another for selling] and differing measures, both of them are detestable and offensive to the LORD.”

- *Proverbs 20:10*

I’m not going to mince my words here: our current financial system is an immoral one. When the system is designed to extract value from its citizens unknowingly while simultaneously redistributing that value to those at the top of the system, that system can be described in no other way than immoral. It’s a very creative form of stealing. And that’s quite possibly what makes it so immoral - it’s hidden. At least bail-ins are overt, and everyone is aware of the theft. But central banking and the manipulation of the currency supply is a hidden theft. It’s like some sort of strange riddle: it’s only known by those who know about it.

At least when a thief breaks in and steals things from your home there’s some evidence of it. But with The Fed’s current scheme, generations pass, and individuals don’t realize why they work hard and save, but it seems like they are getting further and further behind. Their attempt to accrue wealth evaporates before their eyes and they don’t know why.

Bitcoin provides a level playing field and it’s a monetary system by which all rules are known in advance. There’s no hidden back door where the rulers of the network can siphon off value to enrich themselves, unlike our central banking systems around the world.

Thinking Outside of the Box

Why do we accept these bad systems? Because it’s what is presented to us. We fall into cognitive dissonance because we tell ourselves things like, “If it was so bad, someone would have already done something about it.”

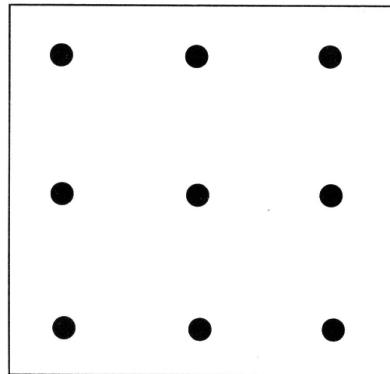
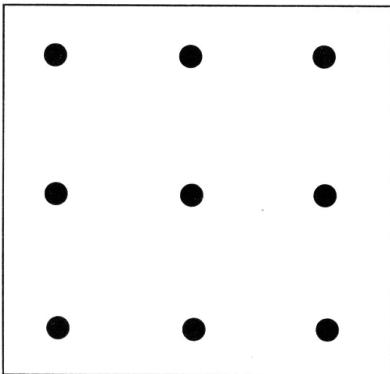
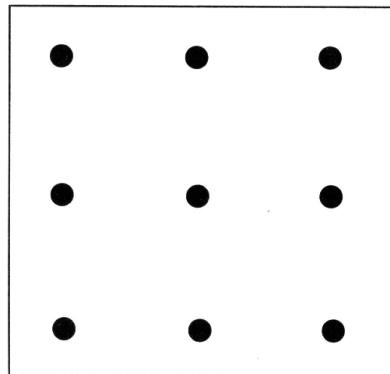
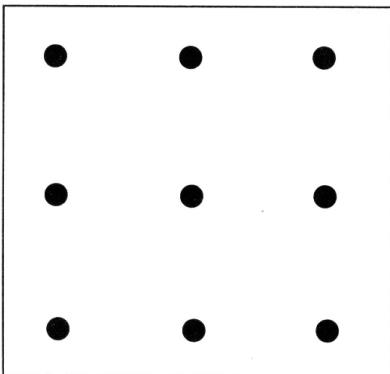
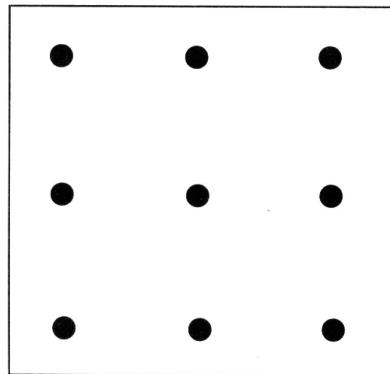
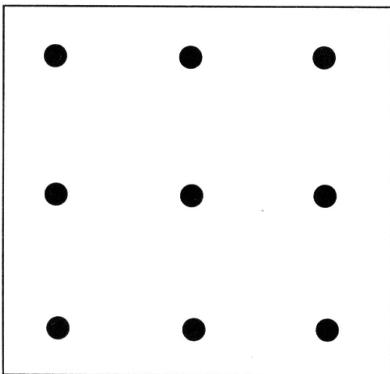
Here's the secret: those who have discovered the scheme are using it to make themselves wealthy. Those that understand The Fed's mission to devalue the currency are individuals that do not hold very much of their wealth in the currency. They buy assets with it. It's a common misconception that billionaires have billions of dollars in cash. In fact, millionaires and billionaires keep drastically less in cash relative to their overall wealth than the average American. The average American keeps about 33 percent of their wealth in cash while a typical billionaire keeps less than one percent of their assets in cash⁽²¹⁾.

The average person takes what they are presented with at face value. Some see the truth but are too scared to act against the status quo. People are fickle and would rather fail with everyone else than succeed by going along the path less traveled. Warren Buffett famously spoke to this point:

"Failing conventionally is the route to go; as a group, lemmings may have a rotten image, but no individual lemming has ever received bad press."

Warren Buffett stated this quote very tongue-in-cheek, but he tapped into the psychology of the typical individual. People are afraid to think outside of the box and fail because then they look like the arrogant fool that thought they knew better than everyone else.

Do you know where the term "think outside the box" comes from? It comes from an old IQ test where participants were tasked with connecting nine dots with only four lines. Give it a try on the next page. I left several boxes in case you need multiple attempts.



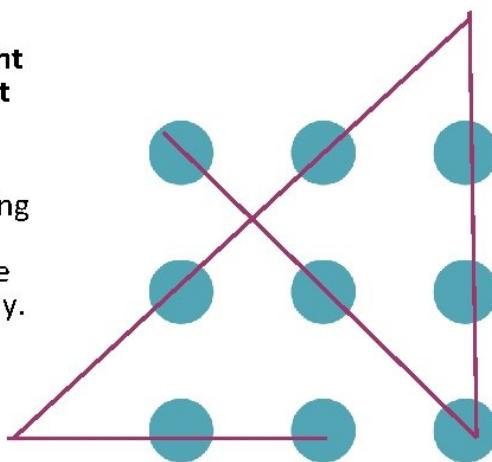
For most people this seems impossible. Those who were able to solve it realized the lines could go outside the box of 9 dots. Most participants probably imagined there was a rule that you could not go outside of the box. Or maybe it just didn't cross their mind. But either way, those that thought unconventionally were the ones able to get to the truth and solve a problem few others could.

The same thing is true with our financial systems. Those who just want to run the rat race like everyone else will also be subjected to the same disadvantages as everyone else. Those who understand how the financial system is rigged will use it to their advantage and, in the case of what I call the Bleeding Heart Capitalist, some will use their resources to help others make the transition to a more fair and equitable system.

Fixation: The Nine-dot Problem

Use four straight lines to connect the nine dots.

Solving this requires escaping fixation by thinking outside the box. Literally.



Chapter Eight:

A Brief History of Currencies

& The Inflation Formula

“The further you look into the past, the further you can see into the future.”

- Winston Churchill

“Inflation is as violent as a mugger, as frightening as an armed robber and as deadly as a hit man.”

- Ronald Reagan

Throughout history, all fiat currencies have been intentionally devalued, usually to fund war or public works projects. This process is known as debasement and refers to metal money of the ancient world. Money always starts in a relatively pure form of metal whether that is gold, silver, or copper. The money supply can honestly be expanded as mineral deposits are found and the supply of gold, silver or copper can be increased. This is a fairly slow and expensive process. There are high costs associated with mining and there is a bit of luck involved in finding these metal deposits so their value can be extracted.

The desire for kings to wage a war or expand public works projects was inhibited by this slow process of mining to increase the money supply. So, the option for the ambitious king (which is true for many of the monarchs in recorded history) is to debase their currency. This means that instead of a pure gold coin, they could make it 90

percent gold, and 10 percent copper. As needed, they could change that to 80 percent gold, 70 percent gold and on and on.

As I mentioned earlier, Athens was the first to do this with their gold coins. They began to debase them by adding copper into the coin. They are the first historical record of a government deficit spending and they did this to fund their war against Sparta (the Peloponnesian War)⁽²²⁾. While Athens was the first recorded nation to do this, they certainly weren't the last. Famously, 16th Century England debased their currency to fund economic expansion after the Black Death. The Greeks, the Romans, the Weimar Republic, and many other nations throughout history have fantastic histories of destroying their economies through the debasement of their currency.

“Inflation is a very serious subject, you could argue it’s the way democracies die... eventually the whole Roman Empire collapsed, so (the current situation) is the biggest long-range danger we have, apart from nuclear war.”

- Charlie Munger,
Vice Chairman of
Berkshire Hathaway

US coinage used to be gold and silver coins and their value was based upon their actual monetary metal weight. Now our coins are made from much cheaper metals like nickel. They essentially have no value as metal, rather, their value is simply declared by the government (fiat).

The opening statement of this chapter was “Throughout history, all fiat currencies have been intentionally devalued.” That is a factual statement, and the word “all” is not used in hyperbole. It's a statement that should not be overlooked. In the same way that the press and various other experts of 1912 said that the Titanic could not sink, likewise there are plenty of people that say the United States Dollar is too strong to ever go away. But let me open up this chapter with this fact: according to the St. Louis Federal Reserve's own data, it took the US 200 years to print its

first \$1T. The next \$1T was printed in only eight years. And most shockingly, according to the St. Louis Federal Reserve's own data, from 2014 through 2020 an astonishing \$10T has been printed⁽²³⁾. Eighty percent of all dollars ever printed were printed in the last 22 months⁽²³⁾.

Ultimately, these are estimations because The Fed is not transparent with these numbers. You may notice that massive government spending has happened across both Democrat and Republican regimes. This is because, while the political elite may disagree on some issues, they are in alignment when it comes to centrally controlled money. Both parties have shown a propensity for spending. Because of this, I believe those who say the US Dollar is unsinkable share a Titanic level of naivety.

Currency debasement is such a commonplace event that there are even economic laws that describe its components. One such law is known as *Gresham's Law*: Individuals will spend the common thing first and will hoard the uncommon or rare thing. Only spending it as a last resort. This happens every time a government debases its currency. As money is debased, some citizens will choose to hold onto the purer forms of the money and will only spend the less pure forms. This creates a problem as the coins that are marked by the government as supposedly being worth the same amount actually have different market values. One coin of 5 Dinar might be worth that face value while another 5 Dinar coin with a higher gold content might actually be worth 10 Dinar on the streets. Since fungibility (interchangeability) is one of the necessary features of a reliable money, this creates a huge problem for a country's sovereign currency.

Skeptics have said since the inception of Bitcoin that it will not be used as currency for one reason or another. Originally, they said because it was worthless. Nowadays they say it's because it's worth too much. To some degree, this latter statement is currently true. Many HODLers do not like to spend their BTC because it is an appreciating asset. This makes it less likely to be used as a day-to-day currency.

I am of the opinion that this isn't going to be a perpetual problem and that it is just simply Gresham's Law playing out. Individuals want to spend dollars like a hot potato because they know they are constantly diminishing in value. But, as governments go in the direction of Central

Bank Digital Currencies (CBDC's), individuals will opt for decentralized currencies as a medium of exchange. Gresham's Law will be overpowered because many citizens will choose to opt out of their government's CBDC and only use it when absolutely necessary (to pay taxes). These people will find so much value in open payment systems that they will desire to pay and be paid in Bitcoin.

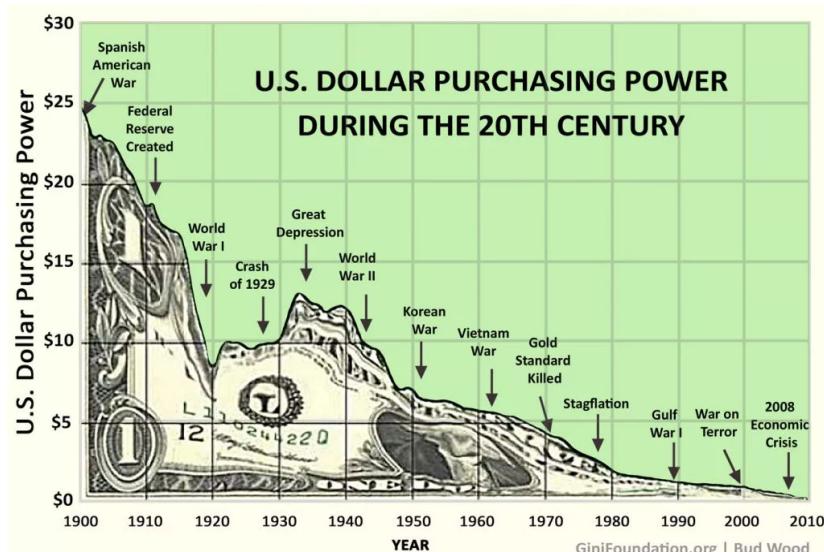
Control of currency has always been of great importance to governments and the elites that pull the strings of society. This concept is summed up well by President Garfield:

“Whosoever controls the volume of money in any country is absolute master of all industry and commerce... And when you realize that the entire system is very easily controlled, one way or another, by a few powerful men at the top, you will not have to be told how periods of inflation and depression originate.”

- James Garfield,
20th President
of the United States

As we discussed in earlier chapters, inflation is not a bug in the central banking system, it's actually a feature. Those that control the supply of money are at a huge advantage over everyone else because they get to decide who gets access to this free and/or cheap capital. There are various mechanisms through which the Federal Reserve allocates easy capital to those on the inside, and these are covered in great depth in G. Edward Griffin's book on the creation of The Fed called *The Creature from Jekyll Island*. That book is highly suggested reading. If you are learning about Bitcoin because you are interested in its liberty-minded components, or you are learning about it because you are interested in it as an investment, it's fundamentally important to understand that the US Dollar system is designed to devalue.

Notice on the chart below that the sharpest drop in the dollar is directly after the creation of the Federal Reserve. Since the Fed came into existence in 1913, USD has lost 98 percent of its value.



According to a survey conducted by Kitco News (an investing research news site), nearly 1/3rd of Americans believe that the US dollar is backed by gold⁽²⁴⁾. This hasn't been true for more than 50 years. On August 15th, 1971 President Nixon took the US (and by extension the rest of the world as most currencies were tied to USD) off of the gold standard. In a press conference, President Nixon stated,

"I have directed Secretary Connally to suspend temporarily the convertibility of the dollar into gold or other reserve assets, except in amounts and conditions determined to be in the interest of monetary stability and in the best interests of the United States."

President Nixon's liberal use of the word "temporarily" reminds me of another famous quote by economist Milton Friedman,

"Nothing is so permanent as a temporary government program."

As discussed in prior chapters, we can be assured that the US dollar will continue to devalue and, in all likelihood, devalue at an increasing rate because our currency system and debts have hit a critical mass. It's of great value to understand how inflation works. It's not a super complicated concept, but there's more to it than most people expect.

Many people, even many academics, believe that inflation is just a function of money supply (printing money). That is not true. If that were the case, then inflation would always be directly proportional to the increase in the M2 currency supply (the supply of US dollars in circulation). For example, if the M2 currency supply went up 80 percent throughout the Covid Crisis, then one would assume that inflation would be at 80 percent. Or at least it would be a fixed ratio that is proportional to the increase in currency supply. But this is not the case. The formula to determine inflation is as follows:

(Currency Supply x Velocity)

The Value of All Wealth.

Money supply = all the currency in circulation.

Velocity = how fast the currency changes hands.

Value of All Wealth = this is a giant number. It's the cumulative value of all the assets and services in an economy. It's the combined wealth of all the citizens of a country.

So basically, inflation is a function of how much currency is in circulation, how fast it is changing hands divided by how much total wealth can potentially be purchased with that currency. If the supply of currency goes up but the country also begins to equally produce more goods and services, then we shouldn't see inflation. If currency supply goes up but people hoard it and do not spend it, then we will not see inflation. Inflation will begin to get out of hand when the supply goes up, individuals begin to spend their currency quickly, and there is no real increase in the amount of goods and services within that economy.

This begs the question, "Who are the winners and losers from inflation?" This is a very big question that really requires a much more in-depth answer, but for the sake of brevity, I will shorten it here. If you would like to study this topic more, Jens O. Parsson's book, *Dying of Money: Lessons of the Great German and American Inflations* covers this topic in great depth. But essentially, the acolytes of Dave Ramsey, the savers, get crushed. Those holding their savings in cash are the biggest losers from inflation because they hold the very item that is in crisis.

Counter to conventional wisdom, the ones that make out like bandits are those with fixed rate debt such as a mortgage or a business loan (it is important to understand that we are talking about fixed rate debt and not some variable rate of debt that can increase with inflation). By 2021 standards, a \$3,000 mortgage payment is a very high mortgage for the average person. But even during "standard inflation" times of 2-3 percent, over the course of a 30-year mortgage, three percent inflation compounded annually means that by the end of your mortgage, your payment has become 59 percent *less expensive* on a real basis (real basis means "accounting for inflation"). This means that a \$3,000 per month mortgage payment 30 years from now would feel like a \$1,770 payment today.

Now, when we add in the seven percent rate of inflation we are currently experiencing in the US (these are based on the "official" Consumer Price Index [CPI] numbers, but many professional money managers state that they treat inflation on their capital as though it is currently 15 percent), over the course of a 30 year mortgage your mortgage would become 87 percent less expensive - meaning that a

\$3,000 per month payment 30 years from now would feel like a \$390 payment today.

At 15 percent inflation your mortgage becomes 99.5 percent cheaper over that 30 year period. A \$3,000 mortgage payment 30 years from now would feel like a \$15 payment today. In the event of a true hyperinflation (50 percent month over month inflation), fixed rate debt essentially becomes free in the matter of only a few months; completely wiping out any debt that you, students, businesses, or the government has.

This fact is why Robert Kiyosaki, the author of one of the best-selling books of all time, *Rich Dad, Poor Dad*, says that his poor dad saved while his rich dad got wealthy by taking on debt. This is counterintuitive to general financial wisdom and may be another indicator of why our system is immoral - the fact of the matter is, those who take on cheap fixed rate debt gain wealth while those who do the responsible thing and save, get robbed.

Above I mentioned the CPI. The CPI number is a very important statistic to understand because it is one of the indicators used to manipulate the public and obfuscate what the true price fluctuations are in our economy. In the 1970s and 80s, the CPI was a legitimate indicator that tracked the rise or fall of the prices of goods and services that are reflections of a typical American lifestyle. Things like food, toothpaste, vehicles, and cost of living are calculated each year and compared to other years. This makes sense. It's helpful to know that in 1975 the cost of toothpaste was 25¢ and in 1976 it had risen to 26¢. A 1¢ increase on a 25¢ item is a four percent rise in price. Economists perform this same calculation on a bunch of different items and then average them out to come up with an inflation number. Sounds good.

The problem is that the way CPI was calculated up until the 1980s (a time when inflation was very high) is not how we calculate the CPI today. Economists use all sorts of statistical tricks to doctor the numbers to say whatever they want - after all, these numbers drastically affect the economy, so there's a lot riding on what they say.

“There are 3 types of lies: lies, damned lies, and statistics.”

- Benjamin Disraeli,
British Prime Minister, 1749

One of the most common tricks used to doctor these numbers is accounting for what is called a “similar living standard”. Sticking with our toothpaste analogy, up until the 1980s, the CPI looked at, for example, what a tube of Crest Toothpaste was in one year, and compared it to the cost of Crest toothpaste in the following year. Today, if Crest toothpaste goes from \$2.00 to \$2.20, they don’t count that as a 10 percent inflation in toothpaste. The way they can make inflation magically go away is by comparing Crest toothpaste from last year to the generic brand from this year. So as long as the generic brand is only \$2.00 this year, then the CPI can statistically show a zero percent inflation in toothpaste.

Unfortunately, this wouldn’t be taking into account that the generic toothpaste was only \$1.80 the year before, so the fact that it’s at \$2.00 this year is actually an even greater relative price increase (11%). When it comes to our institutions, whether it’s public health, economics, or something else, we always need to dig into the data because unless we analyze it, statistics can be very deceptive. If we look at these statistics with our investor hat on, it can give us an advantage when it comes to making decisions.

One of the pernicious motivations for suppressing the CPI reinforces my point about the immorality of our financial system. Since the US has a lot of welfare, socialized medical coverage, and other entitlement programs, the country has a massive cost to payout every month and year. The CPI is the key indicator that is used to justify how much those receiving these entitlements get. If inflation goes up, then these recipients get more.

If inflation is actually at 15 percent but The Fed can say that inflation is only at three percent, then the government only has to increase their payouts by three percent and they get to retain the

difference of 12 percent. This is just one more way that those who run the corrupt monetary institutions take advantage of the poorest and most vulnerable in society. Sadly, many people misguidedly vote for entitlements to help those in need, but then also vote to maintain the status quo that is ultimately doing more harm than good to those very same people they wished to help. That's why clarity on this matter is necessary so we can vote accordingly and make genuine change that results in better opportunities for everyone.

We've all grown up in a world where inflation exists. So, we assume it's a law of nature or that it's simply the way currency inherently works. That's just simply not true. Inflation is a symptom of fiat currency, not sound money. In ancient Rome, before their gold money was debased, we have records of the wages for soldiers being consistent for over 300 years when the wages were paid in pure gold. But as soon as the currency began the process of debasement, while the wealth of the nation did not increase, soldiers' wages had to perpetually increase to keep up with the increased supply of currency. The velocity of this currency also increased because, like Gresham's Law says, people will quickly spend the new debased currency rather than their old pure money. The citizens recognizing that their currency is being debased is the catalyst for significant velocity and then inflation.

Currency supply can and should increase over time, consistent with the growth of the population. I shared this quote from Milton Friedman earlier in the book, but it bears repeating here since we are discussing a healthy currency supply rate of increase:

"I would specify that the Reserve System shall see to it that the total stock of money so defined rises month by month, and indeed, so far as possible, day by day, at an annual rate of X percent, where X is some number between 3 and 5. The precise definition of money adopted, or the precise rate of growth chosen, makes far less difference than the definite

choice of a particular definition and a particular rate of growth.”

Friedman’s point was that a healthy monetary system has transparency and consistency so that citizens can know what to expect. It’s part of the unfair advantage of the elites that they get to control the currency supply and hide the rate of growth of currency from the rest of us. It’s like playing a game where one player knows the score and the other one doesn’t. Knowing the score gives that player a huge advantage. It tips the scales so that the wealthy get wealthier, and the poor get poorer.

This is where a huge part of my passion for writing this book comes from: to help people understand how to rebalance these unfair scales by investing in assets that don’t play by the same tilted rules. Inflation is a hidden tax that is only thrust upon those who don’t know about it. Progressive politicians consistently talk about “taxing the rich”, but those same politicians vote for big spending policies that cause this hidden tax, which ultimately only targets the poor and middle classes. As a Bleeding Heart Capitalist, I look for free market solutions that benefit everyone whether those individuals are aware of it or not.

“Inflation is buy-now-pay-later, and the cost comes due enough later that the causal connection between the purchase and the price is unclear.”

- Jens O. Parsson,
*Dying of Money:
Lessons of the Great German
and American Inflations*

Lord William Reese-Mogg and James Dale Davidson made an interesting prediction in their 1997 book *The Sovereign Individual* regarding this rebalancing of the scales⁽²⁵⁾. Over twelve years before Bitcoin, they wrote the following:

“In the Information Age, individuals will be able to use cyber currencies and thus declare their monetary independence. When individuals can conduct their own monetary policies over the World Wide Web it will matter less or not at all that the state continues to control the industrial-era printing presses. Their importance for controlling the world’s wealth will be transcended by mathematical algorithms that have no physical existence. In the new millennium, cybergold controlled by private markets will supersede fiat money issued by governments. Only the poor will be victims of inflation and ensuing collapses into deflation that are consequences of the artificial leverage which fiat money injects into the economy.”

If the dangers of inflation have not been made clear enough, let me emphatically state that inflation is theft. At its most benign it is a gradual robbery that slowly extracts value from the poor and unsuspecting and redistributes it to the wealthy and those that understand how the monetary system works. To illustrate inflation at its worst and most evil, let's briefly look at the history of West African Millefiori Beads (glass beads used as currency). In the closed economy of West Africa where glass producing technology was limited, glass beads were a reliable form of money.

When Europeans entered the economy with their advanced glass blowing technology, they were able to produce exorbitant quantities of glass bead money that flooded the West African economy and destabilized it by triggering a hyperinflation. As the tribal leaders were battling economic problems they had never encountered before (because they hadn't experienced inflation prior) the African slave trade was born as Europeans were able to inexpensively purchase people from these economically struggling tribes. At its best, inflation is theft, at its worst it is something far more evil.

By leveraging the principles of Game Theory, we can use the information covered in this section regarding the motives of government

and central banks. Our opponents in this game (The Fed) are printing currency at a pace that is guaranteed to cause inflation and the velocity of money is quite high because people are beginning to recognize our currency debasement - we even understand The Fed's purpose in doing so - because the US government has taken on a debt which is only payable if the currency dramatically inflates. Aside from seeing those factors, we can look to history and see with 100 percent certainty that fiat currencies fail. There is no historical precedent for any other outcome. Using this information to our advantage helps to inform our next move by finding a form of money that is hard, limited in supply, and rules based. Bitcoin fits this bill perfectly.

“Currency is to the economy what blood is to the body. Money is to currency, what oxygen is to blood... Now imagine someone has sucked all the oxygen out of the room and in the corner an oxygen mask drops down. That oxygen mask is Bitcoin.”

- Michael Saylor,
Founder and CEO of Microstrategy



The Effects of Compounding Inflation

what happens to a \$100 item
after 10 years of inflation?

2% inflation

7.5% inflation

15% inflation

Hyperinflation
(50% per month)

Year 1 = **\$100**

Year 2 = **\$102**

Year 3 = **\$104.⁰⁴**

Year 4 = **\$106.¹²**

Year 5 = **\$108.²⁴**

Year 6 = **\$110.⁴¹**

Year 7 = **\$112.⁶²**

Year 8 = **\$114.⁸⁷**

Year 9 = **\$117.¹⁷**

Year 10 = **\$119.⁵¹**

Year 1 = **\$100**

Year 2 = **\$107.⁵⁰**

Year 3 = **\$115.⁵⁶**

Year 4 = **\$124.²³**

Year 5 = **\$133.⁵⁵**

Year 6 = **\$143.⁵⁶**

Year 7 = **\$154.³³**

Year 8 = **\$165.⁹⁰**

Year 9 = **\$178.³⁵**

Year 10 = **\$191.⁷²**

Year 1 = **\$100**

Year 2 = **\$115**

Year 3 = **\$132.²⁵**

Year 4 = **\$152.⁰⁹**

Year 5 = **\$174.⁹⁰**

Year 6 = **\$201.¹⁴**

Year 7 = **\$231.³¹**

Year 8 = **\$266**

Year 9 = **\$305.⁹⁰**

Year 10 = **\$351.⁷⁹**

Month 1 = **\$100**

Month 2 = **\$163.²¹**

Month 3 = **\$266.³⁷**

Month 4 = **\$434.⁷⁵**

Month 5 = **\$709.⁵⁵**

Month 6 = **\$1,158.⁰⁵**

Month 7 = **\$1,890.⁰⁴**

Month 8 = **\$3,084.⁷²**

Month 9 = **\$5,034.⁵⁶**

Month 10 = **\$8,216.⁸⁸**



The Effects of Compounding Inflation

what happens to a \$10,000 savings account
after 10 years of inflation?
[in terms of lost value over time]

2% inflation

7.5% inflation

15% inflation

Hyperinflation
(50% per month)

Year 1 = **\$10,000**

Year 2 = **\$9,803.⁹²**

Year 3 = **\$9,611.⁶⁹**

Year 4 = **\$9,423.²²**

Year 5 = **\$9,238.⁴⁵**

Year 6 = **\$9,057.³¹**

Year 7 = **\$8,879.⁷¹**

Year 8 = **\$8,705.⁶⁰**

Year 9 = **\$8,534.⁹⁰**

Year 10 = **\$8,367.⁵⁵**

Year 1 = **\$10,000**

Year 2 = **\$9,302.³³**

Year 3 = **\$8,653.³³**

Year 4 = **\$8,049.⁶¹**

Year 5 = **\$7,488.⁰¹**

Year 6 = **\$6,965.⁵⁹**

Year 7 = **\$6,479.⁶²**

Year 8 = **\$6,027.⁵⁵**

Year 9 = **\$5,607.⁰²**

Year 10 = **\$5,215.⁸³**

Year 1 = **\$10,000**

Year 2 = **\$8,695.⁶⁵**

Year 3 = **\$7,561.⁴⁴**

Year 4 = **\$6,575.¹⁶**

Year 5 = **\$5,717.⁵³**

Year 6 = **\$4,971.⁷⁷**

Year 7 = **\$4,323.²⁸**

Year 8 = **\$3,759.³⁷**

Year 9 = **\$3,269.⁰²**

Year 10 = **\$2,842.⁶²**

Month 1 = **\$10,000**

Month 2 = **\$6,666.⁶⁷**

Month 3 = **\$4,444.⁴⁴**

Month 4 = **\$2,962.⁹⁶**

Month 5 = **\$1,975.³¹**

Month 6 = **\$1,316.⁸⁷**

Month 7 = **\$877.⁹¹**

Month 8 = **\$585.²⁸**

Month 9 = **\$390.¹⁸**

Month 10 = **\$260.¹²**

Chapter Nine:

Digital Asset Investment Principles

“Be fearful when others are greedy and greedy when others are fearful.”

- Warren Buffett/Charlie Munger

Here is the opportunity that lies before you: what if you could go back to 1994 and not just buy internet stocks, but instead buy bits and pieces of the internet itself? What we’re talking about here is a paradigm shift of that magnitude. But what makes this seismic shift different from the internet is that regular people, for the first time ever, are able to get in before the major institutions. Institutions have been handcuffed by a lack of clarity from regulators. This has kept them from fully diving into the asset class. The beautiful thing is that it has left the door open for individuals like you and I to frontrun them.

It’s critically important to know what we are talking about when it comes to the financial decisions we make. Nolan Gouveia, Professor of Business at California Baptist University echoes this sentiment:

“Whether it be digital assets or investing in general, only invest in what you fully understand. There is a lot of money to be made, but it is never a good idea to follow the hype without understanding the fundamentals.”

Thus far we have walked through different elements of Bitcoin to gain a fundamental understanding of it from a technological standpoint. This helped us to understand that Bitcoin and crypto are for real and here to stay. What has been discussed thus far as well as what follows is not investment advice. These are investing principles and a contextual framework for digital assets. For those looking to venture into the digital asset investment space, as well as those already in it that are looking to broaden their perspective, the following are critical elements to first consider.

Crypto is the first new asset class in 315 Years

Bitcoin is something special. This is evident by its novelty as a technology, but it is also illustrated in the fact that Bitcoin and digital assets are the first new asset class in over three centuries. Simply put, an asset class is a grouping of comparable financial assets. The five major asset classes are stocks, bonds, cash, commodities (like gold or oil), and real estate.

The last time an asset class emerged was when the first official bond was issued by a national government. The Bank of England issued this bond in 1694 to raise money to fund a war against France. This bond sale marked the birth of the last new asset class until 2009. As with anything new, there will inherently be caution and skepticism. The old guard will seek to protect their existing investments. But with novelty comes opportunity.

Be willing to be a free thinker and go against the status quo

When it comes to investing in a new asset class, one must have thick skin and be willing to be viewed by their peers in a negative light. The idea of being a free thinker does not mean that one should throw out conventional wisdom. It's exactly the opposite - we should apply conventional wisdom to new frontiers and be ready to follow conventional wisdom even when others are panicking and acting irrationally.

Conventional wisdom does not mean “sticking with the old way of doing things.” That’s a myopic way of thinking of it. Conventional wisdom is having a set of principles and a framework that guide your decisions no matter what context you find yourself in.

Do not look at where things are today. Look at where things will be a year, three years, and ten years from now through the lens of what has happened in the past. If you lived in 1997 and you attempted to base your 10-year investment strategy on the market leaders then, you would have been in trouble. In 1997 America Online was the most visited website and they dominated the tech landscape. That same year, a company called Apple was near bankruptcy. But Apple went on to create a series of technologies that revolutionized the modern world and today their market cap is \$2.69T - making them the world’s largest company, while America Online no longer exists.

There have been plenty of people who saw an opportunity or had a great idea, but they never acted, and therefore they missed out. History does not write about such people.

"Here's to the crazy ones, the misfits, the rebels, the troublemakers, the round pegs in the square holes ... the ones who see things differently -- they're not fond of rules, and they have no respect for the status quo. ... You can quote them, disagree with them, glorify or vilify them, but the only thing you can't do is ignore them because they change things. ... They push the human race forward, and while some may see them as the crazy ones, we see genius, because the people who are crazy enough to think that they can change the world, are the ones who do."

-Steve Jobs,
Co-Founder of Apple

The opportunity we have before us with BTC and other digital assets comes at a point in history where there is a crossroad between a new technology and a set of circumstances (massive government debt, inflation, and authoritarianism in the west) that have uniquely aligned.

The only solution may very well be this new technology. The timing of it all is uncanny.

To help capture the enormity of this juncture in history that we find ourselves at, I'll ask this question again. What if you could go back to 1994 and not just buy internet stocks but instead could buy bits and pieces of the internet itself? And what if there were only 21M pieces of the internet that could be owned by the entire world?

Many people are hesitant to enter the crypto market because they do not want to go against the status quo or the intelligentsia. On one hand they want to strike while the iron is hot but on the other hand, they are concerned about stepping out of line and doing something that could be viewed as foolish, but understand this: the system of fractional reserve banking and central banks with unlimited currency printing is a inherently flawed system - just because others don't see it, doesn't mean that you are the crazy one.

"Men, it has been well said, think in herds; it will be seen that they go mad in herds, while they only recover their senses slowly, and one by one."

- Charles Mackay,
*Extraordinary Popular Delusions
and the Madness of Crowds, 1841*

Just because crypto is a new type of investment does not mean that we throw away tried and true investing principles. We still must consider things like risk vs reward, time horizons, doing your due diligence and market fundamentals just to name a few. If you are entering the digital asset space for excitement, as a way to get rich quick or just to gamble then I can assure you that you will be in for a world of hurt. But if you take a systematic approach to learning and investing, you will greatly increase your chances of success.

Go ahead, step out into the new frontier if you so choose, but just like you wouldn't jump out of an airplane without a parachute, do not proceed into digital assets without intelligent principles. Do not confuse

being forward thinking and going against the status quo with dismissing conventional wisdom.

Watch what they do, not what they say

This is an important principle within crypto, but it's just as important in every other aspect of life. We should always be willing to question mainstream narratives. These narratives are not always bad. Sometimes it might be something genuinely healthy like being encouraged to get 10-15 minutes of sunshine every day since Vitamin D sufficiency has an extremely high correlation with reductions in all-cause mortality. This is a seemingly positive narrative. But other times narratives are meant to intentionally mislead.

The prudent investor must learn to go deeper than the surface. This doesn't just mean reading beyond the headlines; it means looking at any given topic from all possible angles. What are people's incentives to say what they are saying? How is this person arriving at their conclusion? The public likes bumper sticker concepts that are quick, simple, and easy to understand. Is the going narrative a simple answer that is more palatable to the population, while a more accurate answer is not being used because it's more complicated and the population wouldn't like it? None of these questions will give you absolute certainty by themselves, but it's the consistent challenging of the ideas that helps the prudent investor make their decisions.

One of the unique traits of both intelligent investors and early adopters of technology is that they have the ability to think critically and distill things down to their simplest form. Sakichi Toyoda (the founder of Toyota - both a brilliant investor and forward thinker in 1930s automobile tech) illustrates this quality with his famous "Five Whys" technique. His process was simple, anytime someone pitched him something, whether it was an engineering solution on a car or a business proposition, he would always ask "Why?" five times. He was fond of this because he saw that it forced individuals to distill their concepts down to their simplest form and if you could do that, Toyoda believed you could be successful.

A helpful tool for navigating contemporary society would be to ask “Why?” anytime we encounter a narrative. It can sometimes cause us to take a counter-consensus approach to things. Maybe the narrative is “take vitamins” or maybe it’s “Bitcoin is rat poison.” Even the narrative of this book should be questioned. It is through this process we enable ourselves to come to the best solutions possible.

It’s also important to understand that sometimes those who perpetuate a narrative publicly are doing the exact opposite in private. During Covid-19, when California Governor Gavin Newsom *publicly* favored policy for the mandatory masking of all Californians, especially school children, but was then seen dining at a crowded restaurant party without a mask, he illustrated this point very well. This action illustrated the Governor’s true level of concern regarding the virus. His actions showed that he understood he had less than a one percent chance of dying from Covid, but his public policies indicated otherwise. Because of this, one could logically conclude that his policies were not about public health. He must have had some other motive.

We’ve seen this same behavior with respect to Bitcoin. In a 2019 interview with Glenn Beck, financial adviser Teeka Tiwari pinpointed some of the cases of influential individuals who publicly antagonized Bitcoin but privately acted to the contrary. Let’s look at what he pointed out:

- September 12th, 2017
 - Jami Dimon, the CEO of the world’s largest bank JP Morgan publicly stated that “Bitcoin is a fraud” and that he would fire any one of his traders if they bought BTC.
 - Over the next day the price fell by 24 percent.
 - That same weekend the largest buyers of a BTC fund in Europe were Morgan Stanley and JP Morgan.

- January 24th, 2018
 - George Soros, the famous billionaire and notorious British currency manipulator publicly declared Bitcoin a “bubble”.
 - Two months later his \$26B family fund announced they had just received approval to buy Bitcoin.
- February 2018
 - Goldman Sachs report concludes “Bitcoin is going to zero.”
 - Prices fell 27 percent.
 - April 2018, Goldman Sachs announced their new Bitcoin trading desk that they paid \$400M to buy.

One could try to argue that these people and entities had a quick change of heart, but that is not an adequate explanation. Regulated institutions like those listed above must go through months or even years of approval through their boards and regulators in order to start a new venture (such as getting into Bitcoin). In the case of Goldman Sachs, they were actively developing their \$400M trading desk privately at the exact same time that they were publicly denouncing Bitcoin.

Why would they do that? Because when regular people get scared, they sell. They typically sell low. And that’s when these institutions buy; and they buy aggressively.

This kind of behavior is not illegal. There’s even a saying amongst these elite investors: “Get long and get loud.” This means that you use your influence to push a negative narrative in order to get as much of something for as cheap as you can and then once your portfolio is in a position that you are happy with (you’re now long), then you can “get loud” and push the positive narrative, along with your investment, up.

Sometimes, these financial elites sound as if they are bipolar. Let's take a look at Guggenheim Investment Fund Chief Investment Officer, Scott Minard's statements on BTC from 2021:

Bitcoin at \$40,000 in February 2021

"Bitcoin is revolutionary and will go to \$600,000."

Bitcoin at \$64,000 in April 2021

"Bitcoin is tulipmania and a scam."

Bitcoin at \$32,000 in June 2021

Guggenheim registers a fund with exposure to Bitcoin.

Can you see the pattern here? The average, uninformed investor was tossed to and fro like a small boat in turbulent waters during all of this up and down turmoil. They buy high and sell low. They unknowingly pay off the ultra-rich. On the other end of the spectrum there were investors during this time that stayed the course and made life changing wealth by having a steady hand. They were the ones that made principal investment decisions based upon the preponderance of information, not just what some “expert” said, or what popular sentiment was at the time.

Understanding percentages

It is critically important to understand percentages and stats as an investor. It should be required high school reading to study Darrell Huff's 1954 short masterpiece, *How to Lie With Statistics*. Statistics are critical in not only navigating investment decisions, but also for navigating a post 2020 world. Understanding how stats work and what goes into aggregating them will inform the individual as to whether those

stats are helpful or misleading. We will not cover everything in the field of investment statistics here but will touch on a few basic points to get you started.

First up, understand that a 50 percent increase is different from a 50 percent decrease. You may hear someone brag about their crypto portfolio being up 50 percent in the past month but they may not be open and honest about the fact that over the last *three months* they were down 50 percent. This might sound to an outsider as though this person has broken even, but in reality, they are still down a considerable amount. It's kind of like when your friend comes back from Las Vegas and tells you they "made \$200 playing Craps" and yet they failed to tell you that they lost \$400 that same trip playing Blackjack.

For example, if this person started with a \$100 investment and it went down by 50percent, they would be at \$50. If it then went back up 50 percent, they would only be \$75. When an investment loses 50 percent, it requires a 100 percent increase in order to get back to its original value.

In a similar example, let's imagine your \$100 increases by 50 percent you would then be at \$150. From there, if you lost 50 percent, you would be at \$75. In both cases, you gained 50percent at one point and lost 50 percent at one point, and in both cases you would still be at a 25 percent loss from your original investment.

The most you can lose on an investment is 100 percent. There is no limit, in terms of percentages, as to how much your investment can increase. You can lose 100 percent, but you can gain 100 percent, 1,000 percent, 10,000 percent and so on. All this is just to explain this very simple concept that unfortunately many investors do not understand: a percentage loss is more significant than a percentage increase.

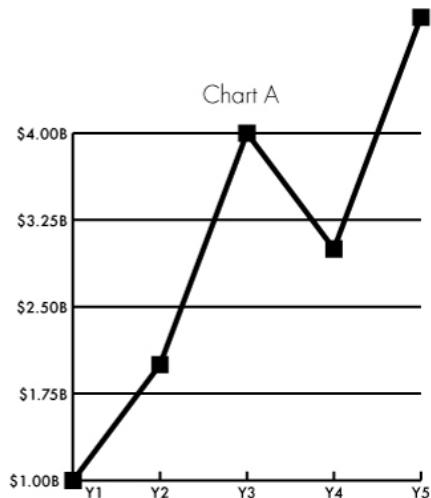
Be very cautious when pundits talk about charts and models. Charts and models can be useful tools to help make sense of the market. But please understand they are not crystal balls. It is all too common to see a headline or a clickbait title that says something to the effect of: "Chart shows BTC is going to the MOON!" or, "Latest model predicts bitcoin's CRASH to zero!"



How To Mislead With A Chart

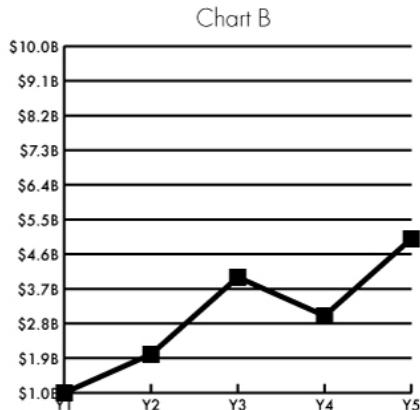
Do you want an explosive growth narrative?

Chart A displays the same data as Chart B. But in this version, we can illustrate "off the chart" growth of an asset or company by simply changing the chart ranges.



Do you want to diminish the growth narrative?

Chart B also shows a growth from \$1B to \$5B over the course of 5 years, and while this chart looks good for whatever asset or company it represents, it displays a much less optimistic narrative than Chart A.



An easy way to discern between those using charts and models sensibly and those using them poorly is the degree of certainty they claim. If a pundit says something to the effect of, “This chart we are looking at shows we could have a rocky road ahead. I’m going to prepare my portfolio for a bearish market because in addition to this chart, we have also received some really negative news lately”, then that indicates they are using their charts to inform their decision *along with* other factors like fundamentals or macroeconomic circumstances.

If the pundit says something like, “My model predicts that BTC is going to \$1M by the end of the month, sell everything and buy, buy, buy!” I would be inclined to question their thesis. If all they have is a model with no other corroborating information, then it’s a very weak model.

The first wave of Covid-19 lockdowns around the world in March of 2020 were predicated on Neil Ferguson’s *Imperial Model*. The model predicted that Sweden, for example, would have 40,000 Covid deaths by May of 2020, and 100,000 by June 2020. Rather than 100,000 by June, the actual number was 2,854. This was not the first time Neil Ferguson botched a model. In 2005, Ferguson had a model that predicted up to 150M people would be killed by the Bird Flu. The Bird Flu’s actual death total: 282.

In March of 2020, politicians around the world cited Ferguson’s Imperial Model as their reason for locking down entire countries. Some responsible news outlets like Del Bigtree’s The Highwire pointed out Ferguson’s failed 2005 Bird Flu model very early on. But that information was suppressed. For everyone else, it wasn’t until several months later that it was discovered Ferguson had been using flawed inputs to achieve his model. Elon Musk stated that Ferguson is an “utter tool” who does “absurdly fake science”. Unfortunately, because decision makers didn’t look for multiple pieces of evidence and instead resorted to a singular flawed model, lockdowns became standard policy. A January 2022 Johns Hopkins study concluded the following⁽²⁷⁾:

“While this meta-analysis concludes that lockdowns have had little to no public health effects, they have

imposed enormous economic and social costs where they have been adopted. In consequence, lockdown policies are ill-founded and should be rejected as a pandemic policy instrument.”

When making a decision, whether it's investing or anything else, one should look for a *preponderance of evidence*. This means that before you make a decision, you should work to find as many pieces of supporting evidence as you can that indicate you are making a high quality decision.

Aside from faulty charts and models, the most common trick in using statistics to deceive or mislead is by confusing one's audience with *relative percentages* rather than *absolute percentages*. Both relative and absolute percentages can be helpful metrics, but it's critically important to always understand which one you are looking at.

In a 2012 press release, the CDC stated that consistent sun exposure increases an individual's risk of skin cancer by 75 percent⁽²⁸⁾. That sounds very scary and makes you want to lather up with sunscreen or just never go outside. But when we look at the actual data from the study, we get a slightly different picture. The study was a very small sample size of 2,000 individuals (1,000 in the test group and 1,000 in the control group). The test group were individuals who regularly went out in the sun. The control group were individuals who rarely went in the sun and when they did, they always used sunscreen.

What the study found was that in the control group, 3 of the 1,000 subjects developed skin cancer. In the test group, 4 of the 1,000 subjects developed skin cancer. For one, this would indicate that sun exposure isn't the only factor in skin cancer since the control group was not entirely resistant to it. Secondly, a difference of one individual in a small sample size can be statistically misleading. Third, how does the study conclude that going from 3 cases in the control group to 4 cases in the test group was 75 percent? They used relative risk to come to a conclusion of 75 percent. To get a clearer picture, most of us would look at what the actual risk difference is (3/1000 vs 4/1000) to get an absolute risk of 33%. This is a vastly different statistical number.

Furthermore, it does not take into account all of the healthy benefits of Vitamin D synthesis via sunshine. Other studies show moderate sun exposure contributes to healthy vitamin D levels and lowers breast cancer risk by as much as 80 percent⁽²⁹⁾. This means that when considering the risk and reward of sun exposure, it's not as simple as just looking at skin cancer risk, especially based upon misleading percentages.

My point here is not to litigate the sunshine and cancer debate. Rather, the point here is to acknowledge that when trying to assess risk vs reward, we must always look at what data is being aggregated into the statistics we are looking at, what type of percentage (relative vs absolute) we are being presented with, and ask ourselves what other variables we should be assessing.

Not all experts are right

“Without education, we are in a horrible and deadly danger of taking educated people seriously.”

- GK Chesterton,
Philosopher & Author

We should judge the accuracy of what someone says by the merit of what they say, not by their title. The argument of authority (for example, saying “I’m right because I’m a doctor”) is among the weakest types of arguments. This does not mean doctors are always wrong (obviously not), but them being a doctor does nothing to validate their point unless they can explain where their informed conclusion comes from.

Prudent investors mold their opinion through the consumption of long form content (reading, podcasts, etc.) rather than having your influences come from headlines and soundbites. Seeking advice from experts is great, but their advice should be one part of your framework. It should not encourage you to become lazy and think that you’ve done your proper due diligence by asking one person.

Traditional TV shows need to cram everything in-between two commercial breaks. Talking heads “win” by throwing out the best inflammatory line rather than by saying something edifying or cogent.

Commit yourself to the discipline of reading. Ray Dalio (the world’s largest hedge fund manager) is a proponent of studying elements of history that have not happened in our lifetimes because macroeconomic events tend to happen in cycles. So, if something hasn’t yet happened in your lifetime, there is a reasonable possibility it may happen at some point in your life. The prudent investor is prepared for such a circumstance and has a strategy they are ready to execute, while the uninformed will be scrambling aimlessly to come up with a solution in real time.

YouTube broadcasts and podcasts have a bad stigma, but think about it like this, CNBC, Bloomberg, and Fox Business have a very polished look to them and are the financial news benchmarks, but they must cover the entirety of financial news. They are jacks of all trades and masters of none. For example, they might discuss Tesla during a segment, but because they have to focus on everything else in the markets as well, their knowledge of Tesla cannot be very deep. By contrast, there are YouTube channels devoted only to Tesla news and discussion.

These YouTubers make their living solely from having a miles-deep understanding of this one company. I’ll watch both formats, but I typically find the insight from the YouTuber is often more compelling than that of the Fox Business or CNBC analysts. There are certainly many low quality YouTube channels, and this goes back to judging the content based upon its merit. Granted, it’s less appealing to say that you got your news from a YouTuber rather than Bloomberg, but that may be a paradigm we see shifting in real time as well.

I find this list both funny and compelling. Next time you are tempted to think an expert is right just because of their title, remember this list:

"A rocket will never be able to leave Earth's atmosphere."
- New York Times, 1936

"When the Paris Exhibition of 1878 closes, electric light will close with it and no more will be heard of it."

- Oxford Prof. Erasmus Wilson

"It'll be gone by June."

- Variety Magazine talking about Rock & Roll music (1955)

"The world potential for copying machines is 5,000 at most."

- IBM's justification for why they didn't buy Xerox

"A wireless music box has no imaginable commercial value. Who would pay for a message sent to no one in particular?"

- The Associates of David Surnov Investments (Responding to the call for investment in the radio, 1921)

"There's no reason for anyone to have a computer in his home."

- Ken Olson, CEO of Digital Equipment Corp (No longer in business)

"Television won't last because people will soon get tired of staring at a plywood box every night."

- 20th Century Fox's Daryl Zanic (1946)

"The horse is here to stay and the automobile is only a novelty, a fad."

- President of Michigan Savings Bank, advising Henry Ford's Lawyer

"Anything that can be invented, has been invented."

- Head of US Patent Office (1899)

I hope experts are right more often than not because I like to gain insight from them. But it is my personal responsibility to not be lazy and go beyond an individual opinion. When you go to the doctor and get an awful diagnosis about your health that requires potentially life-threatening surgery, what's the first thing you do? Get a second

opinion, because your doctor, although she may be brilliant and very good at what she does, might not be seeing the situation from all angles and could have missed something.

The prudent investor hears what experts have to say and balances that information within a larger framework through which he makes his investment strategy.

Bitcoin is an asymmetric asset

A very unique quality of BTC as an investment is that it is what's called an *asymmetric risk asset*. This means that the risk/reward ratio is very broad, in a good way. With any investment, one must ask what the potential downside is versus the potential upside. It's a simple equation that, sadly, many people overlook. This is one of the most important questions you need to ask in your due diligence as a prudent investor.

In a typical year, a large company like Coca-Cola might have an annual stock price increase of 5 percent. Let's walk through some of the considerations you need to make with regard to figuring your risk/return ratio. If you were to invest \$100 in Coca-Cola, at 5 percent it would take you 14.4 years to double your money. What are the chances of Coca-Cola still being in business 14.4 years from now and still growing at least 5 percent a year? Considering that they've been around since 1892 and have a very strong record of moderate growth over that time, I'd say you're making a historically safe investment.

Now let's consider the risk/reward ratio for BTC. If you were to invest \$100, you know that your absolute downside is \$100. Since BTC has only been around since 2009 as opposed to Coca-Cola's 1892, it has less historical precedent and therefore we must consider it riskier. This is where the concept of asymmetric risk comes into play. While the greatest potential downside to your investment is \$100, if we go off the historical record for BTC, then the upside is an annual growth of 178 percent. I don't know if that sounds as substantial to you as it actually is.

While it would take you 14.4 years to turn your \$100 into \$200 with Coca-Cola, with BTC, your \$100 would grow to an astounding \$164,541,593 in that same period of time. I understand that this number sounds preposterous, so please fact check it, but I assure you that it is

accurate. Based upon past performance (which is no guarantee, but it can be used as a guide), your risk is \$100 and the reward is \$164,541,593.

This metric is what has prompted many investment fund managers and public companies to allocate at least a small percentage of their portfolio to BTC. This makes a ton of sense: keep most of your assets in relatively safe investments and put all the risk from your portfolio into BTC because if it does perform, the two percent of your portfolio that is in BTC has the ability to grow your overall portfolio substantially while carrying a very low overall risk.

Everyone's risk tolerance is different. The 64-year-old on the verge of retirement probably wants to carry very little risk - their goal is just to preserve the retirement savings they've worked so hard for their entire life. The 23-year-old recent college graduate who is making a salary but still living with her parents can afford to tolerate quite a bit more risk. If she fails, she can start over pretty easily. If the 64 fails, they essentially have no chance to recover and will spend their remaining days working. As an investor, it is your job to have a very real internal dialogue with yourself to assess your risk tolerance.

Safe investments are great, but the prudent investor wants to find balance between safety and high returns. Asymmetric reward assets are not something that come around every day, but with BTC we have a pristine one.

Buy Picks and Shovels Instead of Prospecting for Gold

In the 1849 California gold rush some prospectors made fortunes and others went broke, but one group of people made money consistently. Do you know which group that was? It was the individuals who set up businesses to sell picks and shovels to miners. For them, it did not matter whether someone struck gold or not, they made money from the mania - a far surer bet than taking a chance by speculating.



This principle has carried on into investing circles. The crypto markets have their fair share of speculation. There are many stories of young people who bought \$1,000 worth of some random coin with their high school graduation money from grandma and it skyrocketed to over \$1M. While these stories are true, they are not as common as one would think. Some people consider the picks and shovels of crypto the physical mining hardware and I guess that makes sense, but those miners are still speculating on which coin they will mine. I view the picks and shovels of crypto as the digital assets that are the building blocks of the decentralized future.

Bitcoin aims to be the digital gold and store of value for the world and may even succeed in becoming the world's reserve currency. Ethereum and/or other smart contract platforms will be the base layer for dApps, DeFi, NFT's and probably many other applications of the technology that we have not yet imagined. Chainlink and/or other oracle protocols will be fundamental in supplying smart contracts with valid, real-world information. These are just to name a few of the picks and shovels.

Why should someone invest in say, ETH, as opposed to speculating on one of the many DeFi coins that are built on top of Ethereum? Because you may or may not pick one of the winners in the

DeFi segment of the market, but by buying ETH, you have essentially made a bet on the entire space. You don't really care which particular DeFi project wins, you just want them to develop on top of Ethereum so your coins have utility and demand. It's like investing in an index fund rather than individual stocks.

When deciding which digital assets you want to invest in, it's important to ask what their fundamental use case is. Does the coin even serve a purpose? Or are you just investing because you have an inclination or a hot tip that the price will go up? If the answer to the second question is yes, just realize you are speculating. When an asset serves an actual purpose and is even currently being used for that purpose in the real world, you can be confident that you're investing in the picks and shovels rather than just panning for gold.

Understanding market capitalization

Market capitalization is a critical piece of data that you must understand when investing. Simply put, market cap is the total value of all the coins the project has. You can calculate market cap by multiplying the current price of a coin by the total number of coins. For example, if you have a crypto project with 100 total coins and each coin is worth \$10, that crypto project's market cap would be \$1,000.

The market cap is the key metric that tells you how "cheap" or "expensive" a coin is. You can have an individual coin that costs \$10,000 (AAA Coin) that is actually "cheaper" than a coin that costs 10¢ (BBB Coin).

Allow me to explain. Let's say there are only 1,000 AAA coins in the world (\$10,000 per coin x 1,000 coins = \$10M market cap). BBB Coin could have a circulating supply of 1,000,000,000 (10¢ per coin x 1B coins = \$100M market cap). The 10¢ coin has a higher market cap so therefore it is actually a more expensive coin in terms of potential return on investment. If you invested \$100 in AAA Coin and \$100 in BBB Coin, the same amount of money would buy you a relatively higher portion of the total supply of all coins in existence on the AAA Coin network. One last way to say this is that \$100 is a greater percentage of a \$10M market cap than it is of a \$100M market cap.

One of the common misconceptions and fallacies within crypto is for investors to be tempted to buy a coin with a lower per coin price because they think that means it's a better deal. Some may have heard that in the early days of Bitcoin that a single BTC was worth less than \$1 and they may be assuming that this new coin could grow in value to something comparable to BTC's price. This simply isn't true. If you are tempted to buy a coin purely because its per coin price is inexpensive, please go to coinmarketcap.com and look up the circulating supply and then check that against Bitcoin's circulating supply; you will find there are orders of magnitude more of that new coin in the world than there are BTC.

In 2021, two of the most popular cheap cryptos to buy were Dogecoin and Shiba Inu. Both coins were created for satirical purposes, but along the way they went viral, and people began investing real money into them. Most investors lost tremendous sums of money on them. From personal experience, I found that most people who invested in them did it because they "could get a lot of coins for not very much money" and "if it ever got to \$10 per coin I would be a millionaire". Dogecoin, for example, has a circulating supply of over 132B coins and this number increases by 5B every year. In order for Dogecoin to get to \$10 per coin, its market cap would have to get to well over \$1.32T, which is over 213 times greater than its market cap at the beginning of the year. To put it lightly, this is a long shot. Hopes of Dogecoin getting to \$10 are based on "what ifs" rather than fundamentals.

In addition to these cheap coins being created for satirical purposes, they have other flaws such as incredibly high concentrations of their coins being held by a relatively small group of people. If one of the core values of crypto is decentralization, then it makes sense to strive for a decentralized concentration of holdings. Below, I have created a chart that shows the concentration of wealth in Bitcoin and Ethereum compared to Dogecoin and Shiba Inu.



Concentration of Coin Holdings

*as of 11/12/2021

"expensive" Coins



Bitcoin



Ethereum

Top 10 holders - **5.28%**

Top 20 holders - **7.25%**

Top 50 holders - **10.55%**

Top 100 holders - **13.33%**

Top 10 holders - **22.12%**

Top 20 holders - **26.40%**

Top 50 holders - **32.11%**

Top 100 holders - **38.32%**

"cheap" Coins



Dogecoin

Top 10 holders - **40.53%**

Top 20 holders - **47.49%**

Top 50 holders - **55.96%**

Top 100 holders - **61.74%**



Shiba Inu

Top 10 holders - **64.26%**

Top 20 holders - **71.70%**

Top 50 holders - **78.74%**

Top 100 holders - **80.84%**

There's a famous saying amongst entrepreneurs: "I'd rather have 50 percent of a watermelon than 100 percent of a grape." The human brain likes to think in terms of *whole coins* so it's perfectly understandable to prefer having 1,000 coins of a project rather than .05 of a coin from another project. But it's important to understand that the prudent investor does not think this way. The prudent investor looks for value, not a vain measurement such as "Well, at least I've got lots of coins!" Having many coins means nothing if they serve no purpose and are worthless.

Developing A Strategy

In this section I will share my own personal strategy for how I perform my due diligence on whichever digital asset it is that I am considering investing in. The exact details of your process can vary, but it's critically important that you have a process. You would be surprised how many people invest significant sums of money and have no rhyme or reason for what they do. Having no strategy is a recipe for investing disaster.

Conventional investment wisdom states we should be *value investors*. Simply put, this means finding an asset that has intrinsic value which is greater than the current market price. This concept should be the core to your entire strategy. Your due diligence process should be an effort to find investments that have an inherent value that is greater than what the asset is currently selling for.

Here is my process:

I. Is it predicated on the greater fool theory?

The greater fool theory means that you know an asset has no inherent value, but you're buying it in the hopes that someone else will pay you a higher price. You are essentially hoping there's a greater fool somewhere out there. Aside from the moral implications of this, it is just bad investing.

II. Don't buy an asset within at least 2 weeks of hearing about it.

Even if a friend gives you a hot tip and tells you that ABC coin is going to the moon this week, you must resist the urge to jump on it. You will get plenty of these hot tips and more often than not, they will fail to live up to the expectation. I've seen many investors go broke making lots of bets on projects they didn't take the time to understand.

A two-week period should give you enough time to vet the project and most importantly, to have some time to cool off from the excitement that can cloud your judgment.

You may miss out on an opportunity here and there, but you will save yourself a lot more money overall. Keep in mind that in raging bull markets almost all projects go up so if someone is telling you about a project that went up during one of these periods, just keep in mind that lots of other projects did as well. A rising tide lifts all boats. This fact alone is not proof of a good investment.

III. What crypto asset class does it belong to?

In chapter #6 we covered the various digital asset classes. Including this in your process shows that you can articulate what type of platform you are dealing with. When structuring your portfolio, you should consider what kind of allocations you want from each sub asset class within crypto.

What percent do you want in Bitcoin?

What percent do you want in dApps?

What percent do you want in Oracles?

...Etc.

For example, my portfolio is 60 percent BTC, 25 percent smart contracts, 10 percent oracles, and 5 percent various other digital assets.

IV. What problem does this project solve?

Being able to clearly define the vision and purpose of a digital asset is critical. Good crypto projects have professional websites, whitepapers, and project roadmaps where they present what they hope to achieve (or already are achieving) and how they plan to grow. If you cannot explain why the coin exists, then it probably isn't investment grade.

V. Who are this project's competitors?

Some projects might be total first movers in the space with no competition yet. But most crypto projects are racing against competitors to solve the problem first. Websites like livecoinwatch.com and coingecko.com have tools for looking up similar projects. Competition is not a bad thing when choosing investable assets. This could actually be an indicator that they have a real problem they are trying to solve. But you should ask yourself which project is best equipped to win the race.

VI. What are the tokenomics of this project?

With digital assets, one must consider things like a coin's price, its circulating supply, and its inflation rate. Some projects even have things called "coin burns". Ethereum is one such project that has this feature and what it means is that with every ETH transaction, a small part of a coin gets destroyed, never to be used again. This helps keep the coin limited in supply and thus helps it hold its value and even appreciate over time.

I have seen some projects offer 7,200 percent annual returns via staking (meaning that if you lock up your coins for a period of time to help secure the network, they will pay you a 7,200 percent return paid out in more coins). The problem here is that while a guaranteed 7,200 percent return on ABC coin, for example, sounds great, the inflation rate devalued the coin essentially down to nothing. In this case, the tokenomics made

this project a very poor investment. This is a great example of “having a lot of coins” that become worthless because of a fundamental flaw in the project.

VII. What is the centralized counterpart of this project?

Many crypto projects are attempting to solve a problem that a centralized company has already solved, but the crypto project is attempting to do this as a decentralized alternative. Good questions to ask here are things like, “Do people even want a decentralized alternative?” Or, “Is a decentralized alternative superior to a centralized one?” Some businesses may actually be better off left centralized while others are ripe for disruption by blockchain.

VIII. If this project reaches the market cap of its centralized counterpart, what will its coin's value be?

The answer to this question can give you some insight into the potential upside of your investment if the project you invest in captures a significant portion of the market. If you are interested in purchasing a coin for a project that is focused on creating a decentralized telecommunications network, you could look to see what the total value of traditional telecommunication companies are. In this case, telecommunications is a large network.

If you are thinking about investing in a coin for a blockchain focused on decentralized lemonade stands, you might find that even if the prospective blockchain captured 100 percent of the existing market, it wouldn't be worth your time and risk.

IX. Read the Whitepaper and project roadmap.

As mentioned above, reading whitepapers and project roadmaps are critical for making wise investment decisions. Beyond just understanding the project's vision, these resources help you understand more about how the protocol works and the nuts and bolts of the technology you are looking to buy into.

X. Is the team behind it legit?

A good place to start is on the website. This will help you understand more about the team and whether or not these individuals have the capability of executing. Some crypto projects may not even list their team. Satoshi Nakamoto was anonymous, but that does not mean we should just buy into any crypto project with anonymous founders and team members as if that is always a good thing. Most projects will proudly show their team to demonstrate to the public that they have the right people to execute on this vision.

Never put yourself in a situation where you are forced to sell. This means not taking on excessive leverage and not investing beyond your means. Always keep some dry powder (this means always have some cash on the sidelines ready to buy when prime opportunities arise). Make sure you are not spending every last dime and that you are able to cash flow your life. Be prepared to withstand any type of market condition.

There's a strange phenomenon that happens in the crypto markets where fads arise every year or two. In 2017 it was ICO's (Initial Coin offerings - a creative way for tokens to raise funds for their new project but that were ultimately declared securities by the SEC). In 2020 there was "DeFi summer". I believe that DeFi is a critical part of the future, but at the time there was a FOMO (fear of missing out) around DeFi tokens that were sold at ridiculously high prices. In 2021 the craze was around NFT's. Just like fashion, things always return to the core - one generation wears fitted jeans, the next generation wears loose fit, the

following generation wears them baggy and yet the next generation wears them fitted again. So, while blue chip digital assets like BTC and ETH may not be the craze at the moment, inevitably, they will become en vogue again - this is how the cycle has worked each time so far. This means that the best time to buy an asset is when it is not fashionable, and others are looking elsewhere.

This all might be more effort than most people are willing to put into their investment research (it's actually not that much work) but if that's the case, one needs to ask themselves whether they want to be just another basic sheep investor who follows the irrationality of the crowds, or do they want to be a disciplined investor who makes money while they invest in helping to shape the future for the better?

Dollar Cost-Averaging

Dollar Cost-Averaging (DCA) is not a particularly difficult or sophisticated method of investing, but it is tried and true. Most people who put money into their retirement account every month are practicing this method, perhaps without even realizing it. Dollar cost averaging just means that instead of making a large purchase all at once, you make smaller consistent purchases, typically on a weekly, bi-weekly, or monthly basis.

For example, if you had a total of \$10,000, many people would just pick a day and go ahead and buy \$10,000 of BTC. Someone that is DCA'ing into their crypto position would buy \$1,000 every two weeks (or some other regular period of time) until they've spent their \$10,000.

The former is a hit or miss strategy. If the price of BTC goes up then you're feeling good, but if the price goes down it can cause stress and panic. Being down on your investment temporarily isn't a huge problem as prices will likely improve over time, but unfortunately, new investors tend to have weak hands, meaning they sell at a loss because they cannot handle the pressure.

When an investor buys \$1,000 every two weeks, for example, sometimes they will buy high and sometimes they will buy low but over the course of their purchases they will tend to get a nice average purchase

price. No one understands what the price of BTC will be tomorrow, so taking away the pressure of trying to time the purchase perfectly is part of why DCA'ing is such a powerful strategy. If you haven't noticed yet, most of these strategies entail removing emotion and inserting some type of discipline.

So many new BTC investors get caught up on needing to have an entire coin. This thinking is what leads people to other projects where individual coins cost less, which may or may not be a good idea. Rather than thinking in terms of an entire bitcoin, tailor your thinking to consider Sats, the smallest units of BTC. This may help satisfy the psychological desire to "have a lot of something". For \$1, currently, you can get 2,564 Sats! *Stack Sats and Chill* should be the mantra of every BTC investor. This makes BTC accessible to everyone because anyone can hold off on buying a couple cups of coffee and instead put \$10 into Bitcoin and get over 25,000 Sats. The *chill* part of the mantra describes the relief of pressure that comes with this style of investing.



USD to BTC Unit Parity

*based upon approx \$65,800 Bitcoin

Dollar to Sat Conversion



\$0.01	15 sats
\$1	1,520 sats
\$10	15,193 sats
\$100	152,044 sats
\$1,000	1,520,000 sats

Not every millionaire in the world can have a full bitcoin. There are an estimated 45M millionaires in the world and only 19M BTC currently. This means that many millionaires will even need to start thinking in terms of Sats rather than whole BTC. No commodity in history has had this type of scarcity.

Think of Sats in the same way that a newbie looks at Dogecoin - “I can get 4,000,000 coins for only \$100!!” I believe that in the same way we currently look back on the people who were the first to buy BTC coins for only pennies, when all is said and done, the people who buy Sats will also have a similar appreciation of their investments. It's entirely possible that each Satoshi comes to parity with the penny or even the dollar someday. How amazing would it be to turn every dollar (that's losing a *compounding* seven percent per year) into \$164 or even \$1,646?

The financial crisis that is coming will be the biggest opportunity in history for a transfer of wealth. Whether you just want to be a prudent investor, or you want to be financially prepared to help others, these types of moves need to be considered.

Opportunity cost

Sometimes in investing you are given many choices. Some of these choices might be winners and some might be losers. Beyond just the winner and loser categories there are also *big winners*, *medium winners* and *small winners*. Someone might be proud of themselves for picking a small winner, but what they don't realize is that they could have picked the big winner – therefore, they fell victim to opportunity cost.

Investing in the S&P 500 in 2020 would have netted you an amazing increase of 16 percent! But investing in BTC during that same period would have had a 320 percent annual yield. While both would have been profitable, the opportunity cost of investing in the S&P 500 would have been almost 300 percent. That sounds like a lot, but when you look at it in nominal terms, the difference becomes even clearer.

- \$10,000 invested in S&P 500 would have grown to \$11,600.
- \$10,000 invested in Bitcoin would have grown to \$42,000.

Choosing the S&P 500 actually cost you \$30,400.

This difference is significant over the course of a single year, but the opportunity cost of not being in Bitcoin over the last 10 years would have been a compounding rate of 178 percent per year. If you understand the power of compounding interest, this opportunity is far too high for a prudent investor to ignore. This opportunity cost is only exacerbated by looking at a 10-year scale.

“Good investing is not necessarily about making good decisions. It’s about consistently not screwing up.”

- Morgan Housel,
The Psychology of Money



10 Year Average Annual Compounded Return

*2011 - 2021

\$10,000 investment

S&P 500

13.55% average yield

Year 1	- \$11,355
Year 2	- \$12,893
Year 3	- \$14,640
Year 4	- \$16,623
Year 5	- \$18,875
Year 6	- \$21,432
Year 7	- \$24,336
Year 8	- \$27,633
Year 9	- \$31,377
Year 10	- \$35,628



178% average yield

Year 1	- \$27,800
Year 2	- \$77,284
Year 3	- \$214,849
Year 4	- \$597,280
Year 5	- \$1,660,438
Year 6	- \$4,616,017
Year 7	- \$12,832,527
Year 8	- \$35,674,425
Year 9	- \$99,174,902
Year 10	- \$275,706,228

How to know if the market is going UP or DOWN

How do we know when the market will go up or down in the short term? Do you want the truth? The answer is that no one knows. People act like they do, but they don't. News programs will have an "expert" on that called the last market crash or the last market peak, but have you ever noticed that each cycle it's always a different expert? Of course, someone will make a prediction and get it right. They may even have a good rationale for why they thought what they did, but anyone that tells you they know exactly where the market is headed in a short period of time is probably being a bit too arrogant.

I was the CMO for Atheneum Blockchain for three years and I couldn't tell you what the price of the coin was going to be tomorrow or the next week. What I could tell you was if we had some new development or had onboarded some new set of users. If that was the case, we could assume that news would cause the price to go up over a period of time based upon utility or speculation. But this was fundamental analysis, not investment mysticism. And even then, this wasn't always a reliable way to forecast the price.

Seeing market cycles allows us to step back and see a much bigger picture. Market cycles have been a fairly reliable indicator thus far about long term price action. With Bitcoin, in particular, we have this incredible scarcity that only needs a little bit of worldwide demand for it to see massive price appreciation. Obviously, I have no insight as to what will happen to BTC tomorrow, but the arc of Bitcoin's trajectory seems to bend toward adoption and growth and therefore, long term price appreciation based upon supply and demand.

Having a long time horizon

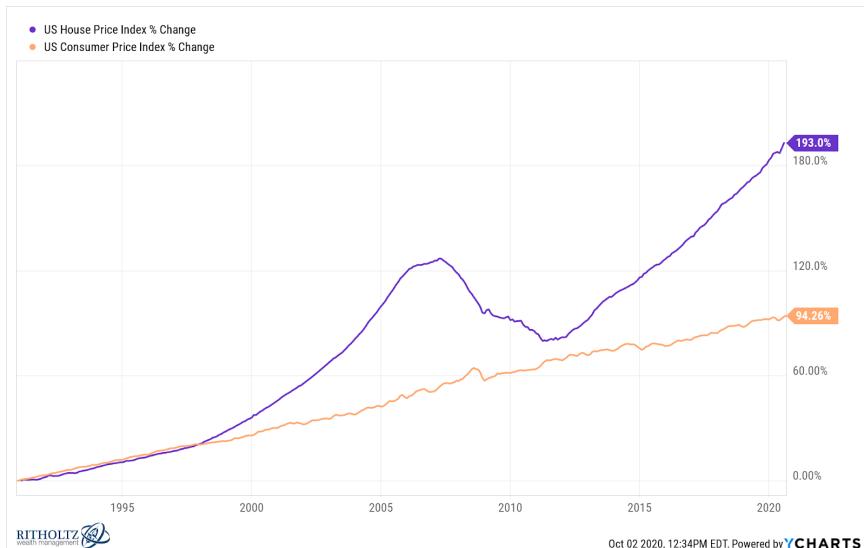
Historically, no one has lost money on BTC if they held it for four years or more. Does that sound strange if you've heard stories about people losing fortunes in crypto from market crashes? The truth is that you only lose money in USD if you sell. You never lose your BTC when you hold. This usually happens because someone was either in a position where they were forced to sell, or they were nervous about the market conditions and decided to sell at a loss. This is why it's so critically

important that you never overextend yourself and put yourself in a position where you can't ride out the turbulence.

There's a well-known investing adage about having a long investing time horizon: "*Time in the market is more important than timing the market.*" Having a long time horizon is a wonderful way of covering any small investment mistakes one makes. For example, if you bought at the very peak of the 2017 BTC bull run in December, you could have sold soon thereafter for a 70 percent loss, or you could have toughed it out until December of 2020 and realized an increase on your investment. If you held for another six months after that, you could have realized as much as a 200 percent gain.

In housing, the only people that really got crushed in the 2008 financial crisis were those who bought at the peak, later lost their job, and were forced to sell. Anyone who bought their home five years or more prior to the collapse were still at a higher home value, even at the bottom of the crash.

Anyone who bought at the absolute peak of the housing bubble in 2007 would have had their mistake erased if they just held until 2016 when home prices surpassed their previous all-time highs. Continuing to hold from 2016 until 2022 would have garnered returns as high as 50 percent on many American homes from their 2007 peak bubble prices.



In 1972, a group of researchers set out to conduct what became known as The Stanford Marshmallow test. The point was to test the life outcomes of individuals that displayed a propensity for delayed gratification when they were children. In the experiment, kids could either have one marshmallow now or two in 15 minutes. Through a series of follow-up studies, researchers found that children that waited had better life outcomes as measured by SAT scores, income levels, educational attainment, body mass index, and other life measures.

It seems there is a universal law that favors delayed gratification and a willingness for long time horizons; whether it's marshmallows, real estate, or BTC.

Part of having a long time horizon allows you to act like a sniper rather than a soldier on the ground. Being an investment sniper allows you to be removed from the immediate chaos of the moment, but you are also able to take advantage of great buying opportunities as they arise. As a crypto investor, you should be more excited by the bear markets than

the bull markets. These are the conditions for buying and preparing your portfolio for the next impulse to the upside.

To go back to Warren Buffett's quote about lemmings (those that follow the crowd), bull markets simply reflect what value the lemmings who still believe in the dollar, place on BTC. Bear markets are where the lemmings are doing lemming stuff and they sell their position at losses. This is where the prudent investor buys. Both bull markets and bear markets are driven by these lemmings (the average investor) and their manias. Baron Rothschild of the famed Rothschild banking dynasty had this to say about whether or not he favored buying in bear markets:

“Buy when there is blood in the streets. Even if it is your own.”

Adam Smith concluded that the “Invisible Hand” (the forces that move markets) does not like it when things are very good or very bad for very long. Just know this: markets correct. They correct to the downside when things get too good and correct to the upside when things get too bad. This is why the wealthy know with 100 percent certainty when to buy - they buy when there is blood in the streets. This isn't easy to do because it's counter to our emotional state. It's scary to buy in bad markets. But, as we have discussed throughout this chapter, the prudent investor learns to trust pre-determined principles and discipline rather than emotion.

Avoiding FOMO: Creating Disciplines for what you invest in

“Discipline is doing what you hate to do, but nonetheless doing it like you love it.”

- Mike Tyson,
*Former Heavyweight World
Boxing Champion and
Philosopher*

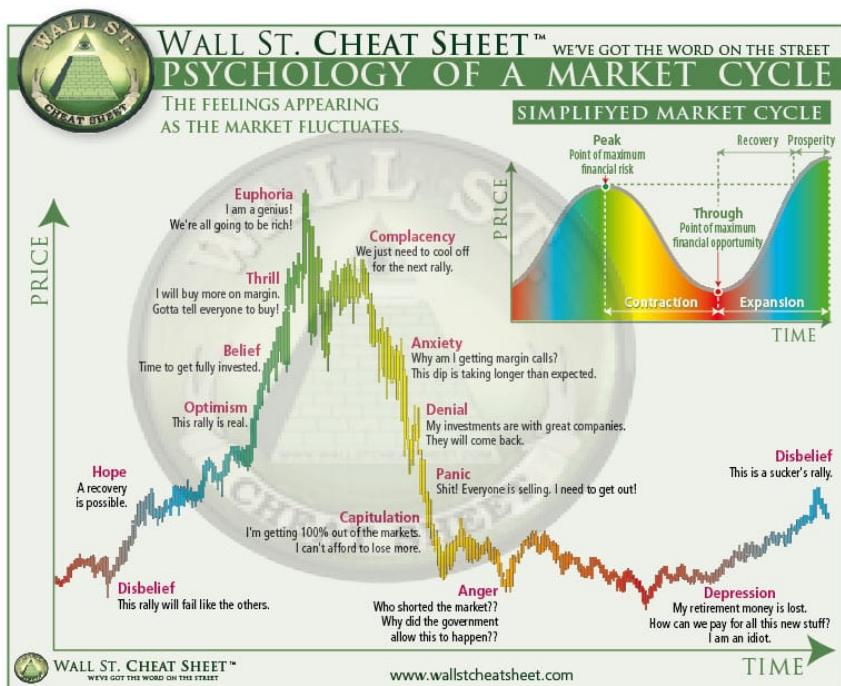
I believe more people have lost money in the crypto space because of FOMO than due to any other reason. We see other people getting amazing returns and then we do a quick calculation of our own finances and realize that if we had just invested all our money in the same way that person did, we would have completely changed our financial future. These daydreams and “what ifs” can be very dangerous and are not productive.

The most important rule about manias and markets is to instill discipline and strategy. Markets *will* make people very emotional, the last thing one should do with money is make emotional decisions. Having a plan and pre-determined investing principles is a must.

One thing crypto investors often overlook when considering a project to invest in is whether the project is growing and gaining market share. New crypto investors seem to cite things such as “If this goes up 10x, I’ll be happy!” or “If this new coin does what BTC did, I’ll be able to retire early” rather than analyzing the project fundamentals.

I like to remind people of what Jeff Bezos said at the 20th anniversary of the public offering of Amazon. Reporters said, “Wow, the stock was so volatile for so long. How were you able to hang in there?” Bezos responded by saying, “Well, I was more focused on users and revenue growth.” One of the world’s wealthiest people got to where he is, not because he was focused on price, but because he was focused on fundamentals and whether a problem was being solved or not.

I find the chart on the following page is a very apt illustration. If you’ve ever been through a crypto or stock market investment cycle, you will be very familiar with these psychological stages. I find this chart helpful because I like to occasionally audit the market and try to pinpoint which phase we are currently in. This gives me a general sentiment as to which way market forces will be pushing.



Jeff Bezos's investment strategy worked out incredibly well because he had high conviction. He believed in what he was doing. You don't have to become married to your investments. Sometimes there is a justification for selling an investment where fundamentals have changed. But a valuable principle in investing is to stay true to your strategy. Do not look for the exits as soon as market forces are doing something you don't like. Have a plan and be ready to ride through some turbulent space. In crypto, if you can bear the downside of the market, you get to enjoy the fruits of the market upside unlike any other investment; one that has the ability to build stratospheric wealth. We opened this section with a quote from Mike Tyson, so it seems fitting to bookend with another one of his quotes.

Despite the appearance of his brutish fighting style in the ring, Tyson is a very intelligent individual. In the ring, as in investing, one

must be prepared to have their gameplan challenged, and you must be willing to have the highest of conviction in order to push through.

“Everyone has a plan until they get hit in the face.”

There will be good times and bad times in your investing journey. How will you react when you get hit in the proverbial face?

When is the perfect time to sell?

To me, the answer is very clear here: Never. This isn't investment advice for you, this is my personal stance. I have spent hundreds of pages in this book making the case for why bitcoin is a pristine asset and perfect money. In my opinion, the question shouldn't be “When is the right time to sell?” Rather it should be, “Why would you ever sell?”

This doesn't mean that I plan to just always HODL all my BTC forever. I told my wife in 2013 the plan that she agreed to and that we still stick to today: we will use our BTC when we can buy things with it. I spend my BTC often to support the crypto ecosystem. I don't plan to spend a big portion of my BTC though, until it has reached a wider adoption because at that point, I will be able to buy more stuff with it.

I think people ask about when the right time to sell is, because they think of digital assets like they think of stocks or traditional investments. Ironically, most people don't sell their stocks very often, and instead, store their wealth in those stocks for decades until they retire. Once someone retires, they may sell those stocks to pay for their expenses. I personally think of BTC in the same way. Maybe not when I retire, but I will store my wealth there and use it when the time is right. But unlike stocks, I won't have to sell my BTC to use the proceeds, I will be able to just directly buy things with it.

The paradigm of traditional stock trading has people thinking about getting in and getting out of digital assets. Let's face it: the idea of making money by sitting in *front* of two monitors with charts and graphs all over and getting to quit your day job sounds really cool. For me, the only experience I have with losing money in crypto is by day trading.

There are people who do this professionally, but they have incredibly sophisticated software and deep capital that allows them to play the game differently than you or I can.

Sure, buying something low and selling it once you've recouped your initial investment and then some is a safe way to do it. I have no problem with that. But I just come back to the idea that what I'm trading back into is the US dollar - a toxic asset. I have a difficult time wrapping my head around selling sound money for fiat currency.

The foreword of this book was written by my good friend Erik Goodin. His story of paying off his mortgage only several years into a 30-year loan is an incredible story and I'm so happy for the freedom that his and his wife's prudent investing skills afforded their family. He and I have discussed the pros and cons of paying off a mortgage early. Erik ran a cost/benefit analysis that made perfect sense for his family's situation. Just as I said, I will use my BTC when the time is right. For Erik and his wife Danielle, the time was right. Plus, the capital they freed up by eliminating their mortgage payment has given them the ability to hyperdrive further investments. It was a very smart and disciplined play.

I'm about four years into a 30-year mortgage myself, but have not chosen to pay off my mortgage with my BTC even though my mother badgers me to do so often. I'm about 10 years younger than Erik, so that factors into my calculus. If I were a decade closer to retirement I would de-risk and pay off my mortgage as well.

One of the biggest factors in my calculus has been where I'm seeing the dollar heading and heading fast. Twenty-six years from now, even at a typical 2.5 percent inflation my \$2,500/mo mortgage payment will be the equivalent of a \$1,315/mo payment today. At seven percent inflation, as stated currently by the federal government, my mortgage would be the equivalent of a \$431/mo payment by the end of its term. If inflation is actually at 15 percent, as many capital managers say, then my mortgage would be the equivalent of \$67/mo through the final years of the term. In other words, I don't want to spend dollars that have stronger buying power today when I know that in the years to come, I am *guaranteed* to get a discount.

My thought process here illustrates one way in which an investor can take into account all sorts of factors and consider them through the

lens of a long time horizon. Erik and Danielle's strategy was a prudent one and I believe that mine is as well, although they are the exact opposite strategies with regard to a mortgage. I'm not making some new age point about how "everyone is right". What I am saying is that by taking into account many different variables, individuals should tailor their investing strategies to their own situations.

When you have fixed-rate mortgages or debt, inflation is your friend. I think inflation is bad for humanity, but for those with fixed debt, they benefit greatly. The Germans in the 1920 Weimar Republic experienced a hyperinflation that made their debts worth pennies and essentially cost them nothing to pay off. This is why hyperinflation and debt cycles add to wealth concentration and wealth gaps among the population. Those who have assets, grow their wealth in these cycles, while those who have no assets and only hold currency get robbed and absolutely crushed.

Tom Lee, the managing partner at Fundstrat Global Advisors, made a very interesting observation in the 2017 BTC bull market. His observation should serve as a warning for those who are trying to time the market by constantly buying and selling: 95 percent of BTC's gains in 2017 (from \$900 to \$19,497) came on only 10 days of the year. So, if you happened to have sold and been waiting on the sideline during the parabolic impulse up days, you would have missed out on a 2,166 percent gain.

Some people sell for a short-term financial need even though they would have preferred to hold onto their crypto and let it appreciate. While everyone's financial situation is different, (this is for informational purposes only) it should be noted that if you need cash, you can borrow against your crypto assets. Doing so allows you to access capital while still getting the upside of their appreciation because you still hold the assets. Services like BlockFi are centralized entities that do this while DeFi gives individuals an avenue to access capital in the decentralized markets. This does come with the inherent risk of centralization.

The Power of Compounding... While Compounding

When you buy BTC or any other digital asset, it can appreciate in value like a stock or commodities such as oil and silver. We've shown the power of compounding appreciation already (the chart showing BTC growth over 10 years vs the S&P 500). One unique thing about digital assets is their ability to be lent out to earn additional interest on the asset.

For example, if you chose to hold your BTC on a lending app, you would be lending out your coins for the benefit of generating a passive return. These yields usually pay anywhere from 1-5% but the interesting part is that the returns are paid out in BTC. So, for those looking to stack Sats, this can be a very simple and effective strategy.

What's so cool about this is that you are essentially getting a double compounding effect - you get the appreciation of the BTC you hold, and you generate an investment yield paid out in more BTC. And guess what, that new BTC you just earned also has the ability to appreciate in value.

This strategy for doubling your compounding effect can be done through CeFi (centralized finance) institutions like BlockFi or DeFi protocols where there is no intermediary. For those wanting to employ these strategies, I suggest testing out both with small stakes and then increase it as your comfort and understanding grows.

Understand that these strategies come with risk. CeFi and DeFi can result in a total loss of assets because of smart contract corruption or a company becoming insolvent. By sharing this information I am not necessarily endorsing it.

Avoiding Scams

New technology opens people up to scams because it's uncharted territory and some people throw out common sense. They think something that sounds too good to be true is actually true because they think "that must be how people are getting rich with this stuff." If something sounds too good to be true, it is. BTC goes up in value because its market value goes up just like a stock or commodity.

Many of the scams in crypto are pretty unsophisticated. A common scam can be as simple as someone on Twitter saying, "If you

send me 1 BTC, I'll send you 5 BTC back!" Who would ever do that? Well, apparently a lot of people, as millions of dollars have been taken from individuals with this scam.

I have also seen actual pyramid schemes disguised as blockchain projects. I had one friend pitch me on the crypto project that they "had recently signed up for." I had to tell her that you don't "sign up" and pay monthly dues to crypto projects. The problem is, when people don't fundamentally understand what digital assets are, they are much more vulnerable. If you perform your proper due diligence as we have covered, you will protect yourself from such scams.

Get off zero!

There is something called "paralysis by analysis". Some analysis is critical, but some people can become so anxious that it makes them incapable of making decisions. So, what they choose is to defer. That's fine, but in this case, those people should know that what they are deferring is their opportunity to be a part of what could be the biggest wealth transfer in history.

The easiest way to get started is by investing an inconsequential amount of money. This serves two purposes: 1) it gets you off the starting line and into the race and 2) being invested at any level will cause you to pay more attention to it. If you are mentally having a hard time getting started, take \$5 and buy some BTC and then just don't touch it. Watch it. I think you'll find that the process was easier than expected and totally painless.

Conclusion

Wealth shouldn't be our end, it should be our means. In a university commencement speech, actor Denzel Washington said to the graduating class:

"You will never see a U-Haul behind a hearse. The Egyptians thought you could take your wealth with you but all they got was robbed."

Ask your why. Why do you want to invest in digital assets? Is it because you want to build wealth? Is it because you want sovereignty over your money? Is it because you want to invest in the decentralized future? Is it so you have the resources to support your family and help others? The answer to this question will be a good starting point for developing your investment strategies and discipline.

“The highest form of wealth is the ability to wake up every morning and say, “I can do whatever I want today.”

- Morgan Housel,
The Psychology of Money

Chapter Ten: *Why Does Bitcoin Have Value?*

“I think one of my incredibly big misses of the last 10 years was not buying enough bitcoin... surely, what it (Bitcoin) is telling us is that this is a crisis moment for the Fed. It is a canary in the coal mine. The crypto market is the pure money market and it is telling us that the epistemic closed bubble around fiat money in the US is heading toward some crisis point.”

- Peter Thiel,
Venture Capitalist
Early Investor in PayPal
and Facebook

While this question is less common among the younger generations, Baby Boomers are almost certain to prudently ask the question of Bitcoin’s value, almost verbatim to this: “Bitcoin isn’t anything. It’s not physical. I can’t hold it. So how can it even be worth something?” While younger generations may ask the same basic question of bitcoin’s value, they typically won’t base their skepticism on it being digital, as they default to seeing digital things as valuable. Instead, they usually ask the question because they simply do not understand the value proposition of BTC. That is what we will cover here.

Value Based Upon: The Economic Definition of Price

Most things of value are only valuable because of the worth individuals place on it. If we just want to go by strict economic principles, then something is worth whatever the market says it's worth. Put simply, it's worth whatever someone is willing to pay for it. The most famous economist of all time, Adam Smith famously said:

“The market system generates prices that are ‘fair’.”

Adam Smith believed that everything has a natural price and an equilibrium will be reached in the market. That equilibrium, essentially wherever the price ends up, is a reflection of the good or service's natural price.

Although this is a data-driven way to look at things and this chapter could end here with a brilliant economist like Adam Smith, most people are not satisfied with this as an answer. Therefore, I will attempt to make a more robust case for the inherent value of bitcoin.

The Economics Book: Big Ideas, Simply Explained echoes what Adam Smith had to say:

“The marketplace is the only way to establish price, as nothing - not even gold - has an intrinsic value.”

These authors say there's really no such thing as intrinsic value, there's only something's price in the open market. Gold bugs may not like this, but according to market pricing, gold doesn't have inherent value because although it can be used for some purposes, it can easily be substituted for another metal. In most cases, other metals are stronger and more efficient. Thus, according to market pricing, gold's value comes strictly from what the most recent purchase price of an ounce of gold was.

I believe there are forces that affect the market price, and I am not a strict market economist in the sense that it is the only way to assess value. Gold's value is ultimately derived from its rarity and hardness (difficulty to produce). Gold is a powerful indicator that rarity can justify a sustainable value over thousands of years - through wars, famines, political coups, or any other type of seismic shift in culture. Its rarity has maintained value that transcends cultures, geography, religion, or nationality.

Baron Anne Robert Jacques Turgot (yup, that's all just one person) commonly known as Turgot was a famous French economist who offered another way of assigning value. A common criticism of BTC is that since it has no physical component, unlike other commodities such as gold, it therefore has no utility. This book makes the case for Bitcoin's utility, but let's just let Turgot answer this objection in his terms.

In 1769, Turgot noted that despite water being the most important commodity on earth, you can't buy anything with it. Unquestionably, water has the greatest *utility* of any commodity on Earth. But utility does not correspond directly to value quantified by its price. A gallon of water can be purchased for \$1 and it will sustain your life for a week. A one carat diamond (smaller than the eraser of a pencil) can go for as much as \$12,000, and if it were your only sustenance, you would die within a few days.

Turgot didn't call it this, but I would define this comparison between the value of water and diamonds as *Utility Value vs Beholder Value*. Beholder value leans on Adam Smith's supposition that something is precisely worth what someone is willing to pay for it (beauty is in the eye of the beholder). While utility value seems like a more sensible way to ascribe value to something, Beholder Value will always be a more precise indicator. Utility Value can be an abstract projection about what something should be worth in the future based upon how useful it is (which is susceptible to many different and varying market forces such as supply and demand, difficulty of production, and scarcity). Beholder Value is only realized after the item has been purchased and we know with 100 percent certainty what the market valued it at.

Certainly, there are other very useful commodities, like oil, that are valuable specifically because of their utility to create power. But when we analyze why a commodity like oil is valuable versus the value of water, it points us back to why BTC is valuable. Oil is useful, but it is also limited in supply and difficult to produce. Water essentially has an unlimited supply and is very easy to produce.

BTC has all the qualities that make commodities like gold or oil valuable. It has a large variety of utilities that create demand (as we will cover in the rest of this section), but it is also scarce and difficult to produce. According to the Market Theory of Value, a BTC is worth exactly what today's price is. Unfortunately, looking at value through this lens means that any asset's value is going to fluctuate. At the time of writing, BTC's market cap is \$785B. This means an individual BTC is worth \$41,477. [refresh] I mean \$41,504. [refresh] I mean \$41,899.

This begs the question, what dictates the market price? If you've taken an economics 101 class, then you know the answer: supply and demand. Valuing assets has always been a tricky thing because economists need to predict both supply and demand. Working with two variables is a difficult task. BTC is the only asset in history where we perfectly understand its supply - 21 million. The only variable in this equation is its demand.

While we could go into a myriad of factors that could affect BTC's demand, let's revisit a previous statement by distilling it down to this overly simplistic point: there are an estimated 45 million millionaires in the world. This means that there's not enough bitcoin in existence, nor will there ever be, for each millionaire to have a full bitcoin. In fact, even if they could be evenly distributed only amongst millionaires, then each millionaire would only get about a half of a bitcoin. This simple fact points out how truly limited the supply of bitcoin is in relation to the scope of future demand.

So, while the market price of BTC today is approximately \$42,000, market forces can quickly take it to new heights. And it's very easy to model a path to extravagant market valuations of BTC that are predicated on the real world demand that is covered in the following sections.

Value Based Upon: Bitcoin as Gold 2.0

As we have discussed throughout this book thus far, BTC is like the digital version of gold. Like gold, BTC is scarce, difficult to produce (through mining), and it is not declared money by the state but rather it functions as such because it naturally embodies the qualities of sound money.

I would go one step further and say that BTC is more gold than gold. I say this because while gold has the above stated qualities, some of them are not perfected in gold as they are with BTC. For example, any gold bug will tell you that gold's biggest selling point is that it is very rare. While this is true, we have no idea how much gold truly exists on Earth. This is due to a few reasons: there's no reliable record of all the gold owned. Gold's market cap (the measurement of all the gold in circulation) is essentially an estimate - and it's an estimate that we really have no reliable way of verifying.

Secondly, we have no idea how much unmined gold is still in the ground. Gold is currently about \$1,800 per ounce. If demand went up dramatically and the price shot up overnight to \$3,000/ounce, then gold miners would be highly incentivized to mine more gold. If they produced more gold (increased supply) then this would act as a suppression on the price of gold. The point here is that gold's scarcity can be altered by human intervention.

Thirdly, we have no idea how much gold exists in the universe. While this sounds silly, some gold deposits on Earth are the product of asteroids that entered our atmosphere long ago. Visionaries have even waxed poetic about potentially mining gold from nearby asteroids in the future. This hyperbole illustrates that gold's supply has a myriad of factors that can affect its scarcity.

This is why people in the Bitcoin community say BTC is “more gold than gold.” Gold’s supply is limited to some degree, but it’s not *perfectly limited*. Being perfectly limited is the major advantage of BTC as a store of value - it is directly programmed into the source code for BTC to be *perfectly limited*. You can check for yourself how much BTC exists today, how much will exist tomorrow, and how much will exist

one hundred years from now. The most BTC there will ever be is 21 million. No gold bug can make any such claim with accuracy about gold.

As we covered in the earlier comparison of digital gold to physical gold, BTC won in every category. BTC is far more portable, fungible, and divisible than gold, which essentially means that in addition to the scarcity and difficulty of production qualities that give gold its value, it has qualities that should give it some multiplier over and above the value of gold.

The gold market capitalization (the total presumed value of all gold in existence) is \$11.489T⁽³⁰⁾. Speculators look at the value of gold and ascribe some potential portion of that market cap to BTC. At the time of writing, BTC's market cap is \$785B⁽³¹⁾. That is only 6.8 percent of gold's. A simple way to project BTC's value as a function of being digital gold would be to compare it to various percentages of gold's market cap. So, if digital gold is 50 percent as valuable as physical gold, then BTC's market cap should be \$5.74T (\$302,000 BTC price). If digital gold is 75 percent as valuable as physical gold, its market cap would be \$8.6T (\$454,000 BTC). At a BTC market cap equal to gold's \$11.489T, a single BTC would be worth \$606,000.

I would argue that there is very little historical precedent for an inferior analog technology being more valuable than a more efficient digital version. In fact, the digital versions of a technology often increase the accessibility of the tech to more people and broaden the market. Let's look at something as simple as maps. Before smartphones, maps were certainly very common. Most vehicles would have them in the trunk in the case of an emergency. State line welcome centers sold them in gift shops for travelers.

But if you are old enough to have lived in the time of paper maps, how often did you use it? Maybe several times per year. Maybe a little bit more. Today, digital GPS maps are a stock app on any smartphone and any vehicle. Finding the new local restaurant used to consist of calling the location and asking what its cross streets were. Today, most young people don't even know what a cross street is. It's not because they are dumb, it's because that's not common vernacular anymore. The reason being is that we never have to ask for directions.

We can do a search for the restaurant, click directions, and then get turn by turn directions from our driveway to their parking lot.

Because of this ease of access and simplicity, many people use digital maps daily or even multiple times per day. Then, add in the prevalence of digital maps in the use of commerce and we see vastly more utility. DoorDash, GrubHub, Post Mates, Uber, Lyft, InstaCart, and any other app used in today's gig economy is predicated on the use of digital maps. Digital maps literally created an entirely new industry. We can go one step further to apply even greater value to digital maps by looking at their role in the logistics industry that powers the mega industry of online shopping freight and delivery. Without digital maps, Amazon could not exist at the scale it does. Same day and next day delivery would be impossible.

The seemingly innocuous shift from analog paper maps to digital maps was actually a critical piece of infrastructure that didn't just double or even 10X the use of maps, it made them orders of magnitude more widely used. That means if we were placing an economic value on digital maps vs paper maps, one could argue that digital maps are at least 1,000X more valuable. Not every industry that goes from analog to digital sees this magnitude of growth. But, even in more modest digital upgrades within specific industries, it is not uncommon to see market growths of 2-10X.

This is why I believe that a conservative estimation of BTC's future market capitalization is that it will be twice as big as gold is today. Meaning, BTC's conservative worth is \$22.979T based upon its role as Gold 2.0. That puts an individual bitcoin at an approximate value of \$1.09M. Consider that this example is based upon today's dollar value. So, when we factor in a diminishing dollar value and the potential of BTC actually achieving higher multiples of gold's market cap, we could actually be talking about a market value far north of here - a bold statement in today's context where there are still plenty of naysayers that BTC will go to zero and the idea of a million-dollar BTC is seen as heresy. Not only will I speak heresy then, I will say that I believe when all is said and done, a \$1M BTC will seem like a ludicrously small prediction.

Value Based Upon: The Current Value of Global Money Remittance

Skeptics of Bitcoin like to say it has no inherent value and therefore it is worthless. If I only have two minutes to refute that point, I'll jump directly to this reasoning: Bitcoin is a worldwide payment protocol, and the market proves that that service veritably has value. How so? Because the payment processing industry is one of the largest and more lucrative industries on the planet.

This argument is so compelling because it is data-driven and factual. I'll usually ask a skeptic, "How much do you think the combined value of money transmitting companies in the US is?" They'll usually say that they don't know, but they'll acknowledge that it must be "a lot".

They are correct. It is a lot. The combined market value of the major money transmitters in the US is well over \$2T. Once I tell the person that, I say, "Do you still think money transfer is not inherently valuable? If it's not, why is the world paying trillions of dollars for it? And this is only considering a few of the American companies. This isn't even the entire US market, much less that of the world. So, the answer to your question is that the absolute minimum value of money transmitting is greater than \$2T."

Visa = \$471.13B

Mastercard = \$363.32B

Discover Card = \$36.38B

American Express = \$148.57B

Diner's Club = \$76.93B

Western Union = \$7.81B

Money Gram = \$790.35M

Paypal/Venmo = \$134.31B

Cash App = \$19.47B

Zelle = \$120B

Banking Remittance = \$700B

Total = \$2.07T

*Based on NYSE data.

This point can be finished right there, but Bitcoin is so much more than this and the market is much larger than just the US. The worldwide money transfer market is worth tens of trillions when we add in all payments, bank transfers, business transfer, etc. Automated Clearing House (ACH) alone processes north of \$51T in payments every year⁽³²⁾.

All of this means that human beings have an inherent need to transfer money to survive and flourish. One could argue that if the definition of *inherent value* is to provide something that humans need for a functioning society, then we have a concrete argument here for Bitcoin having inherent value.

We can use \$2T as a base level for what the value of the Bitcoin network should be, but it's important to read through the rest of this chapter to see how this value should actually be many multiples higher because of additional qualities Bitcoin possesses that our current money transmitting systems do not.

There are already incredible amounts of money being transmitted via the Bitcoin protocol. According to a report by Ark Invest, in 2021 Bitcoin's worldwide payment settlement increased by 463 percent over 2020 (\$2.3T to \$13.1T)⁽³³⁾. The report went on to state that in 2021, Bitcoin's settlement volume surpassed that of Visa's.

Using the Bitcoin protocol to transmit money around the globe has some pretty incredible tangential benefits. For example, it eliminates the need for what are called Nostro and Vostro accounts. These words have Latin origins. Nostro means "ours", as in, "our bank's funds that are being held by your bank." And Vostro means "yours", as in, "your bank's funds being held at our bank." Because international bank transfers can deal with enormous sums of money, it's a much more capital intensive process than small value transfers like a Visa credit card or Cash App payment. That's why Nostro/Vostro accounts are required. Ripple's CEO Brad Garlinghouse estimates these accounts hold about \$5T in dormant capital around the world. Dormant capital is money that serves no other job than sitting there for accounting purposes - to help facilitate remittances. Allow me to explain:

If I have a bank in the US and my customer wants to send money to someone in Germany, they would do so via my banking relationship with a German bank. But it's very difficult to send and receive physical currency every time someone wants to send funds, so before the German bank and my bank could ever send funds, we would first have to set up Nostro/Vostro accounts.

My bank would put, for example, \$1B in an account at the German bank (Nostro) and the German bank would put \$1B in an account with us (Vostro). Now that our Nostro/Vostro accounts are set up with the German bank, we can serve our customers. When my customer wants to send \$1,000 to their relative in Germany, rather than our bank mailing them \$1,000 in cash, we simply send a message to the German bank telling them to credit the account of the recipient \$1,000 out of our Nostro account.

They may then have a customer that sends \$500 from Germany to a customer of ours and we would take that from their Vostro account. This goes back and forth with periodic reconciliations between our two banks. What all this means is that because we don't have a payment system that is digitally native (Nostro/Vostro is *digital messaging* with *physical settlement*), financial institutions must allot vast amounts of capital to lay dormant and do nothing other than facilitate these payments.

As a Bleeding Heart Capitalist, this drives me crazy because it is such an inefficient use of capital. Imagine if these financial institutions switched over to the Bitcoin Standard and used actual digital payments. They could instantly unlock \$5T or more of that dormant capital into the world economy! Imagine how many jobs, products, services, and how much wealth that amount of capital could create.

Let's look at one more element of this. Have you ever wondered why Visa and a company like Western Union are not competitors? They both transmit funds, but they serve two totally different purposes: Visa supports merchant settlements and Western Union provides international fund transfers. ACH is a system that allows someone to directly charge your bank account. Venmo is a nifty social app that allows you to easily send funds to your friends. But none of these do what the others do.

Why? Because they have inherent limitations in their operations, and they must specialize in what mode of funds transfer they provide.

Bitcoin combines all these operations into a single protocol.

If qualities like censorship-resistance (covered next) add value to Bitcoin over existing payment networks, then interoperability certainly adds further value. If we were in 1980 and speculated on the potential value of the internet based upon the sum total of the various siloed university *intranets*, we would get a very low estimation of the value of the internet. Each individual intranet may have been worth an estimated \$100,000-\$500,000 to their respective universities (the ability to send emails around campus has some value). If we added them all up, you would get a sum total of something like \$50M. Is the internet only worth \$50M? No, it's worth trillions and trillions of dollars because interoperability adds exponentially more value. So, just adding up the various payment networks probably gives us a dramatically low estimate of the value of the Bitcoin network. We would have to ascribe an exponential value to the internet because of interoperability.

Similarly, Bitcoin being the protocol that links all payment networks into a single standard creates drastically greater free flows of capital (Venmo to Cash App. Cash App to Wells Fargo. Wells Fargo to Twitter. Twitter to your distant relative's lightning wallet in Europe), and so on.

On the Bitcoin payment standard, borders, app limitations, and prejudices will no longer inhibit the flow of capital and that is tremendously valuable to those who seek equality and fairness along with more wealth and prosperity to go around.

Value Based Upon: Censorship Resistance

For many people, especially the Libertarians, censorship resistance is the chief attribute of Bitcoin. In the context of the 21st century, this is for good reason. Throughout this book we have touched on censorship in various forms and how blockchain technology can be

the solution to these problems that balances the scales away from the few and the powerful back in the favor of the people.

In his famous work from 1948, George Orwell speaks to the power of controlling narrative through censorship:

“Who controls the past controls the future: who controls the present controls the past,”

Blockchain has the ability to protect documents from being doctored. It can ensure that medical records are accurate. It can create a system where medical research data is easily auditable, transparent, and free from bias. It can protect individuals against deep fakes. The Bitcoin blockchain is growing its user base everyday as it becomes the foundational protocol for the world's first rules-based, open, and transparent financial system. A financial system free from corruption and the most dangerous form of censorship - financial censorship.

When I worked as the Chief Marketing Officer for Atheneum Blockchain, one of the coolest solutions to a pervasive problem we worked on was creating what we called a Smart Resume. The resume in its current form really isn't that dynamic. It's a piece of paper that is a self-attestation of one's education record, job history, and maybe even some other skills. Yes, there is some amount of verification that can be done like calling former employers. But in our research at Atheneum, we found that 90 percent or more of prospective employers had *never* contacted a school's registrar office to verify an applicant's diploma or advanced degree. Over 50 percent of employers admitted to not calling references or past employers because of the headache of the process (as past employers do not typically make themselves very accessible for unproductive tasks like this).

With a Smart Resume, employers could quickly and efficiently validate employment and education records through the Atheneum blockchain. The vision of Atheneum is to build a platform where anything you learn can be added to your Smart Resume so your resume is a more accurate representation of your knowledge base. For example, I never took a course or got a degree in graphic design, but when I started

my business, we couldn't afford a graphic designer. So, I went to YouTube and watched dozens of hours of videos and learned professional grade graphic design.

If I were applying for a job today, I could put "graphic design" as a skill on my resume, but that would be in the section right next to how many words per minute I type and the section where I say "I'm a hard worker", not in the formal education section, which is a significant distinction. Speaking from an employer's perspective, we don't take that section very seriously because people can basically just write down anything. But with a Smart Resume you could watch video courses on graphic design, pass a test to verify your knowledge, and upon completion, a record of your knowledge would be posted to the blockchain and added to your verifiable Smart Resume for any prospective employer to validate with a quick search.

The idea that someone can show a more accurate and robust representation of their knowledge and skills is a really cool concept, but the fact that these individuals can actually own and protect their own information is quite possibly a much bigger idea.

The idea of censorship resistance goes beyond money. The history of inventions and intellectual property is filled with stories of people stealing one another's ideas. Sometimes this could just be one competitor stealing another competitor's invention, or it could be a large corporation stealing a small individual's idea. In the past, there weren't easy or efficient ways to solve these disputes and prove who was right. If an individual wanted to sue a large entity that stole their intellectual property, they could be drowned in legal bills before they could even get to a verdict.

Being able to publish an idea or invention to the blockchain creates an ordered and verifiable record to easily settle these types of disputes and prove ownership of inventions and ideas.

Developing nations are fraught with property rights disputes. It's not uncommon for corrupt governments to steal property from citizens by simply changing the deeds. If the government forged a deed that said they owned your property, what recourse would you have? None. Putting deeds to property on the blockchain can be one of the greatest solutions

to preserve property and wealth for those that are vulnerable and have very little.

In addition to outright banning and overt censorship, there are also forms of *soft censorship*. These can manifest as shadow banning - where a social media account is not banned, but their reach gets drastically reduced without their knowledge. Soft censorship can also take the form of outright lying about the circulation of specific content (listing a video's view count low when in actuality, it has many more views).

From 2016 until late 2020 a former producer from *The Doctors* TV show hosted the online medical show *The Highwire*. The show broadcast on its own website, but most of its viewers were through YouTube and Facebook. The show hosted interviews with top doctors from around the world. Some of these doctors expressed views that were considered misinformation regarding Covid-19 at the time (information that is now widely considered accurate).

Ultimately, the show was banned from Facebook and YouTube, but before that, it faced some pretty serious soft censorship. While the show was still broadcast on Facebook and YouTube, the average show viewership was about 100,000 views per episode (combined between both platforms). These platforms are the largest social networks in the world and therefore provide a wide base of prospective viewers. In late 2020 the show was canceled by both platforms for distributing “misinformation” and the only place viewers could then view it was by going directly to the Highwire website.

This would be a massive hit to viewership, right? Well, it probably was, but even with this hit to viewership (because most YouTube and Facebook users would have been unaware of the ban), The Highwire published their viewership numbers after a few weeks of website-only traffic. Rather than 100,000 views per episode they were tracking about 1.5M views per episode. The circumstantial evidence seems overwhelming that YouTube and Facebook severely artificially lowered the view counts for these videos. Whether their motivation was to sway public opinion or to reduce the monetization of this content, it

provides another excellent example of the tremendous value that censorship-resistance has in our current context.

While there are many areas where censorship resistance and self-sovereignty of your information will be great tools to preserve freedom and uphold justice, the most important implication of blockchain is its ability to provide a monetary network that cannot be corrupted. No entity can shut down a transaction on the Bitcoin network.

In January 2022, truckers from all over Canada and the US formed what has become known as the Freedom Convoy. The protest eventually grew well beyond just truckers. Thousands of citizens protested in the Canadian capital in below zero-degree weather to protest COVID-19 vaccine mandates. People from all over the world wanted to support the truckers and over \$10M was raised through GoFundMe - an online donations platform. GoFundMe expressed their disagreement with the principles of the Freedom Convoy and quickly froze the \$10M funds. The company initially stated that they would distribute these frozen funds to another charity, but later agreed to refund the donors. Ultimately, this company exercised their ability to withhold payments from a cause that they disagreed with.

In the wake of this censorship, a competitor to GoFundMe called Give, Send, Go decided to step up and promote another donation campaign to raise funds for the Freedom Convoy. The company stated that their business would be devoted to not censoring donations in the manner GoFundMe had. They raised several million dollars. What a beautiful thing that liberty won, right? Wrong. The government of Canada stated that they would force banks to freeze and seize any funds that entered Canadian bank accounts from these donations. Even though Give, Send, Go would be properly distributing the funds, the banks ultimately have the power over fiat. It just goes to show that the more participants there are in a transaction, the more points of failure or censorship there are.

Neither type of censorship would have been possible if the donations had been collected in BTC. This sentiment was brilliantly articulated by the Nunchuk.io team (a BTC wallet software company). The Canadian government made demands for their company to release

info on individuals that use Nunchuk BTC wallets. The Nunchuk team tweeted their response:

“Yesterday, the Ontario Superior Court of Justice sent us a Mareva Injunction, ordering us to freeze and disclose information about the assets involved in the #FreedomConvoy2022 movement. Here is our official response.

“Nunchuk is a self-custodial, collaborative-multisig Bitcoin wallet. We are a software provider, not a custodial financial intermediary.

Our software is free to use. It allows people to eliminate single points of failure and store bitcoin in the safest way possible, while preserving privacy.

We do not hold any keys. Therefore, we cannot freeze our users' assets. We cannot prevent them from being moved. We do not have knowledge of the existence, nature, value, and location of our users' assets. This is by design.

Please look up how self-custody and private keys work.

When the Canadian dollar becomes worthless, we will be here to serve you too.”

Bitcoin has intrinsic value because of its inherent ability to protect against censorship. According to the site 99Bitcoins.com, China has officially banned Bitcoin six times⁽⁵⁰⁾. The net effect is that the Bitcoin network had zero service downtime, network interruptions, or network failures because of this. The world's most capable authoritarian government in the world with vast amounts of AI at their disposal have been unable to hack or censor Bitcoin. The network is simply too strong and powerful.

If individual bad actors, giant mega corporations, and even governmental superpowers cannot stop or censor Bitcoin, then Bitcoin unequivocally has inherent value. In the previous section we calculated the approximate cumulative value all of the US's payment networks at

\$2.07T. Worldwide money transfer is in the tens of trillions. If Bitcoin provides the function of worldwide payment rails but also adds the additional attribute of censorship resistance, then one could justify a 2-10x multiple to that value - making the value of Bitcoin as a worldwide censorship resistant payment network at least \$20T (\$1.052M per BTC).

“The problem whether it’s the Fed, Afghanistan or Covid is that we have these machines that generate consensus and uniformity and not asking dissident questions and as far as I can tell, the hour is late for these institutions and it is more urgent than ever that these voices get heard. If there is a misinformation problem, it is a centralized misinformation problem - coming from the Ministry of Truth (1984 reference)... I can’t help but think that the worst forms of this fake consensus, dangerous centralization of thinking, this Ministry of Truth, they are all the globalist versions... And for this reason, I want to nominate Satoshi Nakamoto for a heroic award and a ticker-tape parade.”

- Peter Thiel,
Facebook's 1st investor
& Co-Founder of PayPal

Value Based Upon: Network Effects

Go to any Bitcoin online forum and you will see the Bitcoin nerds talking about something called “network effects”. This term certainly existed before Satoshi wrote his whitepaper, but the crypto community has taken the ball and run with this concept. And it’s for good reason. Network effects can be used to analyze the growth of things like the internet, smart phones, social media, telecommunications, and more.

There’s a law regarding networks called Metcalfe’s Law. It posits that you can value a network based upon how many users are on it. It states that the value of a network is equal to the square of its nodes. It was originally applied to telecommunications in 1980 - specifically

phones and fax machines. In this example, each phone and fax machine is a node. This absolutely makes sense on its face. If there was only one telephone in the entire world, would it have any value? No, not when you consider that its purpose is to connect you with someone else.

Having two telephones would be infinitely more valuable than one. If you had one and your mother had one, it would serve the purpose of staying in contact with her. But it provides you no other value in terms of contacting anyone else. If your best friend also got a phone, this three node network would have even greater value because now you can rely on it for not only family correspondence, but also social correspondence. If your business associate also got a telephone, your little four phone network would have far greater value because now it has not only familial and social connections, but *economic* connections. Each node (phone) that gets added to the network makes it worth even more to you.

A study that spanned three years by NFX (a tech venture capital firm), found that network effects accounted for 70 percent of the value in tech companies over the last 20 years⁽³⁵⁾. This is a pretty incredible statistic when you consider all the value these companies provide in the form of everything from internet services to social media, to logistics, to smartphones, to the entire app store, and much more. All those companies have an incredibly high worth, and 70 percent of all of that value was due to network effects. The top 100 companies on the NASDAQ (the exchange for the world's biggest tech stocks) have a cumulative value of \$15T⁽³⁶⁾. This means we can put a price on the inherent value of network effects based upon just a portion of the world's tech stocks, that equates to \$10.5T. That's a massive number.

The earlier example of your small telephone network showed that network effects have inherent value. The latter example of tech stocks shows that network effects have monetary value. So, let's apply this now to the Bitcoin network.

Bitcoin is growing at the fastest pace of any network in history. This is not even counting the entire blockchain space. We could merge Bitcoin and other blockchains together to further enhance my point because I believe there will be network bridges between blockchains to further multiply each chain's individual connections. Just like independent university intranets were bridged into the world wide web,

there are currently brilliant minds working toward bridging blockchains - in fact, some are being launched and tested as these words are being written. But Bitcoin itself is growing so quickly that I can still make this point by only referring to it.

Bitcoin is growing faster than the early days of the US highway system, high speed rails in Europe, the internet, and the telephone. Each of those are incredibly valuable in their own right and are major parts of the infrastructure of our modern world. While the transport of people, information, and communications are all very important things, I would argue that the transfer of money is the most important as it is at the core of everything. If a network for sending information is valuable, a network for sending money is more valuable. If a network for sending packages is valuable, a network for sending money is more valuable. You get the point.

The free market has spoken and has said that network effects have substantial social and economic value. Posting things online versus writing them in your journal is worth over \$735.5B (that's just the market cap of the top four US social media firms).

When I think about the implications of network effects in the crypto space, I get very excited because they enable the little guy to have the same tools as the big guys. Without network effects, the little guy simply cannot compete. Let's look at another benefit of network effects.

If you wanted to start a newspaper back in 1940s New York City, you'd better have some serious funding, otherwise it would be impossible for you to compete with the incumbents (NY Times, NY Post, Wall Street Journal, etc.). These companies have what are called *economies of scale*. This means they can reach so many subscribers because they have the infrastructure - journalists, editors, publishing facilities, and freight and distribution relationships, etc. Over time and with vast resources, these companies have built infrastructure that enables their businesses to be profitable. But they have created an environment where it is impossible for the small independent journalist to start his own newspaper company. He simply wouldn't have the tools in place to be successful.

Now fast forward to the 2020s. A journalist can create a website in an afternoon and have their first story published by evening and their

cost would be about \$100. Why could a journalist not compete with the NY Times in 1940 but they can compete in the 2020s? The network effect of the internet has provided an economy of scale by aggregating all the components needed to start a newspaper company - content creation, publishing, and distribution. The upstart journalist has built none of that infrastructure himself, but gets to benefit from all of it.

We have already covered how the various payment systems are siloed and they do not interoperate. You cannot send USD from Venmo to PayPal. You cannot send USD from Zelle to Cash App. Furthermore, you can't send USD from Facebook to PayPal. The reason is that they do not speak a common language. Bitcoin is a base protocol that can enable them all to talk to one another.

Recently, Cash App and Twitter integrated the Bitcoin Lightning Network API (application programming interface) into their apps. Any apps that integrate this API can talk to one another. So, while Venmo and PayPal cannot send USD to one another even though they are owned by the same parent company and are both payment apps, Cash App and Twitter can send payments back and forth. They can even send USD back and forth using BTC as the bridge! In a nutshell, Person A sends \$10 in USD from Twitter, the Bitcoin Lightning Network converts that into BTC for a split second to transfer it along the Bitcoin payment rails to Cash App where Cash App turns it back into USD.

No, these are not even two payment apps that are sending value back and forth, one is a payment app, and the other is a social media app. What is the value proposition of being able to easily and simply send money to your friend from your Venmo account when all they have is Zelle? What is the value proposition of being able to pay your AC repairman from your Strike App when all he has is a bank account? The answer is that this is an incredibly high value proposition. It will make people in the late 2020s pity the antiquated way people had to send money in the early 2020s.

Value Based Upon: Digital > Analog

Recent history makes this point emphatically: digital things are more useful, scalable, and valuable than their analog counterparts.

We see this illustrated in the music industry. The phonograph was invented in 1877 by Thomas Edison and thus the industry of recorded sound was born. It wasn't until 1931 that the first commercially available record was available. This created a new era where you didn't have to watch something live or hear a live radio broadcast to listen to your favorite music. Later, cassette tapes and CD's dominated the landscape by making music storage and playback even more efficient.

The limitation to all these forms of recorded sound was that they were physical and therefore required physical space to store them, move them and organize them. As a child of the 1980s I had the pleasure to grow up during the transition from cassette tapes to CDs. Cassette tapes needed to be rewound. If you wanted to listen to a particular song on an album you had to fast forward to *about* where you thought the song started and then you'd have to wait for the previous song to end, or you overshot it and had to miss the beginning of the song you wanted. This sounds benign, and it was, but moving from tapes to CDs was mind blowing to users because you could skip easily from one track to the next just by clicking buttons.

CDs were the most efficient type of analog media. But by today's digital standard they are incredibly inefficient. The physical element of storing CDs was burdensome. The latest iPhone can hold 25,000 songs. Let's just say that the average album had 12 songs on it. That means an iPhone could hold about 2,083 CD's worth of songs (about 75.5lbs of CDs). Going from analog to digital in music meant you could carry a storage closet worth of CD's in your pocket.

With that physical component comes organization. Not only was it a pain to keep CD albums in alphabetical order on one's shelf, but you also had to ensure that when you switched out discs in your player, the proper CD got into the proper case when you were done with it. In the 1990s it was not an uncommon sight to see a CD collection that had half of the discs in the wrong case. This meant that finding the album you wanted to listen to could be a ten minute quest of opening and closing cases at random until you found what you were looking for. Even when you did find it, you better hope it wasn't scratched or else it would skip constantly and maybe not even work at all.



Many people overlook is how user-friendly music is today. The concept of a music streaming service and access to any song in the world for only \$9.99 per month was not only unfathomable with analog music media, but it just wasn't possible.

Imagine having to go back from Google and DuckDuckGo to encyclopedias. Rather than pulling up a search app on your phone and typing in a question and having the answer in less than 10 seconds, you would first need to either buy an expensive set of books or drive down to the local library. If you even found the book that contained the answer, you would need to browse the pages to find the specific answer to your question. With a search app you have the answer and are on with your day. With encyclopedias, finding the answer took all day.

With the advent of the search engine, the world's information was at anyone's fingertips. This is a far cry from the Middle Ages where only the wealthy and privileged could read, let alone had access to books. It's a far cry from the 1980s where most questions just went unanswered because they weren't worth the time that it took to find them. How quick and efficient are search engines? There are stories of individuals saving someone's life by using a search engine to find a video on how to use a tourniquet to stop bleeding. In addition to extreme cases like that, search

engines allow for incredible amounts of self-training and education on virtually any subject.

Don't know how to change the electrical outlet in your house? You could call the electrician for a \$100 service call, or you could search for the step-by-step directions by a skilled electrician and do it yourself for the few bucks that it costs for parts. Efficiency in search means that now you can not only find answers, but you can build skills.

Encyclopedia Britannica, the preeminent encyclopedia company's highest annual revenue was \$72.9M⁽³⁷⁾. Google, the preeminent search company's highest annual revenue was \$75.32B⁽³⁸⁾. What is the value of digital search vs analog search? According to this comparison, digital search is 103,319 percent more valuable. Some might call that statistically significant.

It's laughable when a Bitcoin skeptic goes on cable news and says, "Bitcoin has no value. It's worth nothing because it is nothing!" I cringe because the anchor never pushes back. Just once I would love for them to retort, "So you're saying it's worthless because it's digital... would you say that physical CD's are more valuable than streaming services? Are you saying that instead of Google, we should go back to encyclopedias? And I'm sure that when you go on vacation that you must have plenty of paper maps on hand because they are so much better than your car's GPS."

One of the lenses through which I view the world, and especially economics, is one of constant analysis. Is popular consensus and expert opinion just plainly the opposite of the truth? What are the possible motivations for what the experts are saying? Do the people that are speaking out have any conflicts of interest? What is the narrative that the masses are being told? Are the crowds being rational or irrational? In the 1950s when everyone's mom and dad smoked cigarettes and doctors said it was good for lung capacity and longevity, it would have served the critically thinking individual well to act counter to popular consensus. This is exactly the way I see Bitcoin and, more broadly, investing in it.

The old guard experts and public opinion say Bitcoin has no value because it is digital. Bitcoin being natively digital is precisely one of the compelling reasons for why it is so valuable. I always find it ironic

when an expert Tweets their disdain for Bitcoin, or a friend of mine texts me to tell me they think Bitcoin has no value. The fact that they are using digital technology to express disbelief in digital currency simply because it's digital, almost seems poetic.

Value Based Upon: *Transportability*

Our modern context in a developed nation paints a pretty jaded picture of the world. Most people throughout the course of humanity do not have the same privilege that you or I have by being born in the time and place that we were. While 2020 quickly ushered in a very different reality, most of us grew up in a time of abundance and freedom and therefore some of Bitcoin's value propositions seem less important.

For example, the reality for 94 percent of Americans is that they have easy access to banking services and therefore can easily participate in the economy. Pitching the idea that Bitcoin means that anyone with an internet connection can be their own bank may not set off the "eureka!" lightbulb for those in the west, but if you lived in sub Saharan Africa, you might think differently.

Similarly, telling someone who lives in a relatively free democracy that BTC is supremely transportable may not make the blockchain click for them. But what if you were a German Jew living in 1930s Germany? New laws being instituted constantly that made your daily existence more and more oppressed would be your context. The need to flee for a better future or even survival was your reality. Because your every move was scrutinized, an escape from the country would need to be covert. Blatantly packing up a U-Haul and then driving across the country for several days would be out of the question. Selling all your possessions for German Marks would be useless if your goal was to go live in Switzerland since Marks would have no value there.

What if you sold your possessions for gold? Everywhere in the world takes gold! The only problem is that gold is very heavy. Even a small net worth would have meant carrying dozens of ounces of gold on your person. That's cumbersome, noisy and quite obvious to anyone who sees you. Furthermore, you live in a society where someone would kill you just because they do not like your race let alone being able to rob dozens of ounces of gold from you. While gold would give you a future

if you could get to Switzerland, your prospects of getting there successfully with all your gold are quite low.

Had Bitcoin existed in the 1930s, it would have been the perfect store of wealth for refugees. One could store their entire net worth by memorizing a few words. There would be nothing for a hot-tempered SS trooper to take from you, nor would a bandit along your journey see you as a target since you would be carrying very little.

Transportability has very real implications in the world today. My church had Christian Missionary contacts in Afghanistan in 2021. When President Biden ordered all troops to be pulled out of the country immediately, Christian missionaries were run out of the country overnight by terrorists. The brave souls that stayed were killed. In addition to missionaries, there were Afghans that aided the US during the war who were also in immediate danger. These individuals didn't have any time to sell their belongings or even take much with them. Bitcoin is undoubtedly relevant in that context.

What is BTC's transportability value to you? Maybe quite low. What is BTC's transportability to a 1930s Jew or a 2021 Afghan? It's literally worth everything they own.

Value Based Upon: Psychological Value

I earned my bachelor's degree in Psychology with an emphasis in Human Behavioral Science. But it wasn't until I fell in love with economics that I saw how psychology affected more than just the individual. Psychology affects markets, it affects politics, and it affects more aspects of your world than you may realize. Have you ever bought the lesser of two menu items at a restaurant even though you didn't want it as much, or perhaps not at all, but you bought it because it was the cheaper option? Have you ever tipped a waiter a little extra just so that they would think you are nice? These are just a few examples of where psychology and economics meet.

There is perhaps no greater intersection between psychology and economics than when it comes to determining the price of something. When you hear about someone paying \$1M for a strange painting, have you ever thought to yourself, "What a waste of money!" One of the best

examples of this is the famous “White Rabbit in a Snowstorm” painting. Imagine how difficult it would be to paint a white rabbit in a white snowstorm... it’s just a blank canvas. But the original and even copies of this silly painting have sold for thousands of dollars each.

Why would such a thing sell for so much money? The answer is quite simple: because someone thought it was worth it. The psychological factors at play for the person that bought the painting are probably not the same psychological factors at play when you or I see the painting. If you’re like me, you might even find yourself frustrated that someone would throw away so much money on something so nonsensical.

One of the most powerful psychological factors in determining worth is *nostalgia*. For example, you own two virtually identical wedding rings - both valued at \$5,000 by the local jewelry store - but one was your mother’s wedding ring, and the other was just a ring that looked like it. If the jewelry store called you a week later to say that they had someone interested in both of your rings, you may be willing to sell the second one for the \$5,000 market price, but when it comes to the one that was your mother’s, you say no. The store may say, “We’re willing to give you \$10,000 for that one!” To you, it doesn’t matter that the going rate for the ring is only \$5,000 and that you will get paid a premium. To you, that ring is worth far more, it may even be priceless to you.

Things have more value over time. We see this in things like baseball cards and even brand loyalty with the type of car one drives. If you’ve driven a Chevy for ten years, then the likelihood of your next car being a Chevy is quite high. You may even refer to yourself as a “Chevy Man” by that point.

I’ve seen this psychological phenomenon play out in my own life with a gift given to me by one of my daughters. When she was in preschool, one of her crafts was to make daddy a bookmark. I love to read, so it was actually a cool gift even though the bookmark itself wasn’t particularly well designed. It had a bunch of scribbles on it and my daughter’s name was nearly unreadable.

When she first gave it to me I thought it was sweet, but I do not like clutter, so I have kept a policy in the house that we only keep her really premium stuff. This bookmark was not her best work, but it was a

valiant effort. I thought I had eventually tossed it out. About two years later I found it in one of my books. I had accidentally kept it instead of throwing it away. Time sure flies and seeing a snapshot of something my little girl made two years before instantly changed my perspective on the bookmark. Now, I wanted to keep it. Now I appreciate the imperfect handwriting on the bookmark because it was so cute compared to her very neat big girl handwriting now, and it reminded me of her as a little girl.

The item itself was not initially meaningful to me, but the addition of time imputed value onto this book mark. I still have the bookmark. Whereas, I had originally intended to throw it away, once its nostalgic value grew, I wouldn't even sell it for a substantial sum. This is because I have a psychological fondness for it.

I believe that Baby Boomers and Gen X have a nostalgia for US dollars. Those dollars have been the gold standard for currency around the world throughout their entire life. They were brought up with the idea of saving dollars trained into them. For Boomers and Gen X'ers, when it comes to a greater psychological affinity for USD or BTC, they will almost always be drawn to USD. It is what they know, the dollar represented the American Dream to them, and they simply have a nostalgia for it because of the element of time.

Millennials and Zoomers on the other hand do not have this same nostalgia. These generations grew up in an era of gaming and having a life online. In game currencies mean something to them. Getting a like on Facebook is a form of social currency. Getting retweeted is important to them. Getting a new follower can make their day. These digital interactions have legitimate value to them.

Boomers and Gen X'ers are digital immigrants. Millennials and Zoomers are digital natives.

So, what are the economic implications from the psychology of a digitally native generation? The most difficult generation to win over and adopt Bitcoin (or any technology for that matter) is the first generation. Why? Because for generations before that there has been an economic status quo. With the status quo comes familiarity, comfort, and nostalgia.

It's most difficult for that first generation because they genuinely have to step out of their comfort zone. But we have already seen the first generation adopt Bitcoin. Millennials have been adopting it widely since 2015. Zoomers in more recent years. We've already broken the ice. Now it's just a matter of scaling up and fully formulating a new status quo.

According to bankrate.com, in 2021, nearly half of millennials (49 percent) are comfortable with investing in crypto assets such as Bitcoin, compared to 37 percent of Generation X and only 22 percent of Baby Boomers⁽³⁹⁾.

A CNBC study had even more bullish findings for Bitcoin. It found more than half (53 percent) have at least 50 percent of their wealth in crypto and nearly a third have at least three-quarters of their wealth in BTC, ETH, and other types of cryptocurrency, according to the survey. The crypto holdings of millennial millionaires stand in stark contrast to older generations of millionaires and that a whopping 83 percent of millennials held at least some digital assets⁽⁴⁰⁾.

Millennials are set to inherit \$30T over the next 20 years⁽⁴¹⁾. If 83 percent (and growing) of that generation store their wealth in BTC because BTC itself has become nostalgically valuable to them, then what can we expect from the Zoomers, a generation that grew up entirely online? When you pair psychological effects with value and a tidal wave of wealth transferred in a relatively short period of time, we can see BTC valuations that would be laughed at for their absurdity by the experts today.

Seeing obscenely high values for BTC is possible when we understand a psycho-economic effect I call *Capital Flow Inertia* (CFI). All this means is that the price of something is more greatly affected when large sums of capital flow into it within a shorter period of time. This dramatic inflow of capital is triggered by some sort of positive psychological phenomenon in the market.

If the same amount of capital flows into an asset but it occurs over a longer period of time, the market has a chance to reach equilibrium and the price will be less affected. Think of this like eating food. If you ate six eggs, a steak, and a stack of pancakes in a single meal, you would feel incredibly sick. So much food in such a short

window has a pretty dramatic effect on you. If you were to eat that same amount of food over the course of a day, your body would be able to process it, the food would settle and you would be ready for more. This is true for markets, too, but instead of all that food in a short amount of time giving you a stomach ache, capital rushing into the market has dramatically positive effects on price. Capital that flows in slowly has time to settle, giving an opportunity for new supply to enter the market and limiting that capital's positive effect on price.

We can think of CFI like we think of inertia in physics. A six-pound bowling ball sitting on a glass plate does no damage to the plate. But a six-pound bowling ball dropped from a 10ft height has tremendous inertia and strikes the plate with enough force to shatter it. It's the same six-pound bowling ball, but the velocity at which it travels changes its effect. This same principle is regarding the effect capital has on asset prices. Let's look at a non-crypto example and then we'll look at an example as it applies to our context in the crypto markets.

Imagine you are a farmer and you have developed a new type of fruit, a cross between an apple and a banana. You name it the Bapple. There's only one tree in the entire world that produces this kind of fruit, and you own it - so the supply is low. You decide on Saturday you are going to open a stand and sell your new fruit. You made a video about your new fruit, and it went viral because the public is fascinated by your novel fruit. But you are unsure if that means the stand will be busy or not. So, demand is uncertain.

You have 100 Bapples. You plan to sell each one for \$5. If you sell all your inventory, you'll make \$500. You open your store at 9am and right away you have a customer, and they buy your first Bapple for \$5. This confirms your estimation that you can sell them for \$5 (this would mean the market capitalization of your Bapples is \$500, as you suspected - 100 Bapples x \$5). After your first customer leaves you see a wave of other customers coming. You can tell these customers are eager. The next customer, seeing the incoming demand as well, buys 80 of them for \$5 each. You realize that you've already sold 81 of your 100 Bapples to only the first two customers and there are at least fifty more people in line.

You decide to raise your price to ten dollars. Unphased by the price increase, the very next eager customer buys nine more - making the market cap of Bapples go from \$500 to \$1,000 ($\$10 \times 100$). Only having 10 left and a sea of customers, you decide to raise the price again. The next customer buys nine Bapples for \$20 each - causing the market cap to jump to \$2,000! The capital is flowing in so quickly that it's causing extreme increases in the going rate of Bapples. You've now sold 99 of your 100 Bapples to only three customers! The line of customers, seeing that you are almost out of inventory, start shouting out prices. "I'll pay \$50 for one." Someone else cries out, "I'll pay \$100!" You reply, "sold!" and gladly sell your last one for \$100.

The demand for your product has so drastically outpaced supply that the price went up with far more force. The last purchase price of \$100 brings the total market cap of Bapples to a staggering \$10,000, although you only received \$820. This was much more than you originally expected. \$820 of incoming capital in a short period of time created a high Capital Flow Inertia (CFI), meaning that only \$820 translated into \$10,000 of value in the market.

Interestingly, when you had sold 99 Bapples, the market cap was only at \$2,000 (last price sold: \$20 x the total 100 Bapple supply). The last sale for \$100 told the world that people are willing to pay \$100 for a Bapple, and this is why the market cap jumped from \$2,000 to \$10,000 ($\$100 \times 100$) based upon only \$100 of new money into the market. Because of a high CFI, \$100 of capital translated into an additional \$8,000 worth of market value.

In a slightly different scenario, let's say that Bapples are much less popular, and you sell them monthly because you have a lot of trees that produce fruit consistently. Each month you have 100 Bapples, but you only sell 70 or 80 of them. The price never goes past \$5 because there isn't enough demand, and you have a high supply. After 12 months you sold \$4,800 of your fruit, but the market cap is still only \$500. The market cap will not increase because the CFI is too low - capital coming in at a slow pace over a longer period of time. In the first scenario, only \$820 of capital came into the market but the market cap grew to \$10,000. In the second scenario, \$4,800 came in but the market cap never surpassed \$500. The difference: Capital Flow Inertia.

This principle was clearly evident in the 2017 crypto market bull run. An estimated \$6B of new capital flowed into the crypto market between August and December of 2017. In August of 2017, the market cap of the entire crypto industry was \$77.78B. New capital of \$6B coming into the market should push the market cap to \$83.78B ($\$77.78B + \$6B$), right? Wrong. Because the Capital Flow Inertia was so high, that \$6B of buying pressure in a short window pushed the market cap to \$326.5B. With \$6B of new funds coming into the market in a very short period of time, \$248.72B of value was created.

To wrap our heads around this principle further, let's look at another example. Let's say there was a new crypto project called \$ABD coin. It has a very small market cap of \$2M. There are 100M \$ABD coins total in the world. This means \$ABD coin's market price is \$0.02 ($100M \times \$0.02 = \$2M$). To keep things simple, let's also say that the coin is only sold on one exchange. You think this coin is going to be the next big thing and you decide you want to buy a lot of it. You go to the exchange and buy up all the orders of the people willing to sell to you at \$0.02. There were only 100 \$ABD coins available to be bought at \$0.02 (meaning that you bought them all for a total of \$2). You see that there are 100 more \$ABD available at \$0.04. You don't want to buy them all, you actually only buy one at \$0.04. Because the last purchase price was \$0.04, this means the going rate for \$ABD is now \$0.04.

You've now spent a mere \$2.04 total, but you single-handedly moved the market price from \$0.02 per coin to \$0.04 per coin. Since there are 100M \$ABD in circulation this means that your \$2.04 increased the total market cap of all \$ABD coins from \$2M to \$4M. Because this market was so illiquid (meaning there were so few coins for sale) compared to how much demand there was, the Capital Flow Inertia was very high and therefore a very small amount of capital disproportionately increased the overall market value to all holders. If this explanation is confusing in written format, please see the illustration below.



Capital Flow Inertia

Market Capitalization: \$2,000,000

\$ABD

Starting Coin Price: \$0.02

Coin Supply: 100,000,000

High Capital Flow Inertia

Hour 1\$ABD available @
\$0.02: 100

\$ABD

Incoming Capital:
\$2All \$ABD @ \$0.02
were purchased.
Market Cap =
\$2,000,000.
(\$0.02 x 100,000,000)\$ABD available @
\$0.04: 100Incoming Capital:
\$0.04One \$ABD @ \$0.04
was purchased.
Market Cap =
\$4,000,000
(\$0.04 x 100,000,000)New Market Cap:
\$4,000,000

Low Capital Flow Inertia

Week 1\$ABD available @
\$0.02: 100

\$ABD

Incoming Capital:
\$2New Market Cap:
\$2,000,000\$ABD available @
\$0.02: 100**Week 2**Incoming Capital:
\$2New Market Cap:
\$2,000,000\$ABD available @
\$0.02: 100**Week 3**Incoming Capital:
\$2New Market Cap:
\$2,000,000**Total Capital Invested = \$2.04****Period of Time: 1 Hour****Market Cap Increase = 100%****Total Capital Invested = \$6****Period of Time: 3 Weeks****Market Cap Increase = 0%**

On a much larger scale, this effect holds true for BTC. There are only about 19M in existence today and it is estimated that at any given time, only about 1M BTC are for sale. Basically, there isn't much BTC out there. But there are trillions of dollars that will be flowing into the market. Many economists make the common mistake of thinking that if \$1T comes into the market, the market cap will increase by \$1T - this means they fundamentally overlooked the Capital Flow Inertia. If that \$1T comes in over a short period of time, it will increase Bitcoin's market cap by many multiples of \$1T. If \$2.04 can make \$ABD coin gain \$2M in value, what will happen to BTC when trillions FOMO into it as everyone around the world recognizes how scarce it truly is? What happens when \$30T is inherited by millennials that have an affinity for BTC and keep over half of their wealth in the asset class?

Value Based Upon: *The First Ever Self-Sovereign Money*

How does it feel to know that you do not control your money? Have you ever even truly considered that? If you have over \$10,000 in a bank account, go and try to withdraw it all at once. It probably won't happen because your bank has all sorts of restrictions in place in the name of "safety": safety for you, and safety for them by ensuring that you are not committing some illegal act. Your bank refers to it as Anti-Money Laundering (AML) regulations.

People who attempted to donate to the Canadian Truckers Freedom Convoy in 2022 found out very quickly that they are not sovereign over their own money. Those who received donated funds had their bank accounts seized. Those donating could be charged with supporting an insurrection - a very serious crime.

What is the value of someone having true financial independence? This is an abstract concept because it is not a data-driven valuation. It's a principle-based valuation. Self-sovereignty over one's money has incredible value to those in countries or villages that regularly switch dictators or warlords. Top-down authoritarianism always targets money first. Having a powerful defense against this in the form of BTC

gives these individuals a tool that those facing similar situations in the past didn't have.

In a world where governments can unilaterally shut down businesses, schools, churches, sporting events, and family gatherings, being solely in control of your own money has an amazing value proposition. At the time of writing, BTC is worth \$40,684. That means that in today's context there are some people around the world who will sell a coin for that price. But what if western countries followed Canada's lead and began to freeze and seize individual bank accounts?

The value proposition changes pretty drastically if that's the case. Then we aren't talking about a speculative value of BTC. Rather we'd be talking about the value BTC has to keep you from having all your wealth taken. Let's say you own one BTC. If I offered you \$50,000 for it, but there was a 50 percent chance that the cash I just paid you could be seized the next day, would you take the offer? What about \$100,000? \$1,000,000? What amount of money would you take for the coin-flip chance that it could all be gone tomorrow because it was seized, and you could have nothing?

In a chaotic environment, sovereignty over one's own money is like insurance. All of a sudden, fiat becomes gambling and BTC becomes the sure bet.

Value Based Upon: Bitcoin as Perfectly Sound Money

What is the inherent value of the only form of money in history that is durable, portable, divisible, fungible, limited in supply, widely accepted, a store of value, a unit of account and digitally native?

By comparison, fiat currencies possess only a few of these properties and the total world's wealth held in them is \$90.4T. If Bitcoin is described as *sound* money, then fiat currencies could accurately be described as *unsound* money. So, we could say that perfectly sound money is worth somewhere north of unsound money's \$90.4T value. I understand that some form of government fiat currencies will likely always exist, so it would be unreasonable to expect that all \$90.4T flows into BTC simply because it's far better, but hypothetically speaking, a

\$90.4T market cap for BTC would translate into about a \$4.3M price per coin. This isn't even accounting for Capital Flow Inertia.

The point here is that serving the function of money is inherently valuable. The world has ascribed a value of \$90.4T to that function. As shocking as it may sound, one could argue that because BTC is better money, it's fair to say that buying BTC for anything less than \$4.3M per coin is a discounted buy. Keep in mind that these points are not intended to offer investment advice, but rather to explore concepts around valuations and to debunk the worn out argument that "Bitcoin has no inherent value!"

Value Based Upon: Being the Most Secure Computer Network in the World

In the battle against unsound money and banking cartels, Bitcoin supporters say that the reason Bitcoin will win is not by having a great offense, but rather, by having a better defense. If a protocol intends to be the base layer for the world's financial system, it better be impeccably secure.

I believe that Chapter 3 pitched a pretty solid case for Bitcoin's security. In a nutshell, Bitcoin is the world's most secure computer network ever. Security is obviously a valuable thing. Billions are spent to secure various networks around the world every year. But the value of security is not solely in what is spent on protecting information, the value of network security is derived from what would be lost in the event of a breach.

Security is an inherent value of the Bitcoin protocol. While it may not be straightforward to attribute a dollar value to this characteristic, it should at least silence the critics that say Bitcoin is good for nothing. That accusation is veritably invalid. The Bitcoin blockchain is inherently valuable, in large part due to its security.

Value Based Upon: The Only Money You Can Take to Heaven

The ancient Egyptians were known for their strange burial practices for their Pharaohs. It was common for Pharaoh to be buried in an extravagant tomb in a luxurious sarcophagus. Within the sarcophagus he would be buried with treasures filled to the brim. The thought was that this great wealth would be carried over with him into the afterlife.

The reality for Pharaoh is that his tomb would be raided thousands of years later. Apparently, his vast fortune never made it to the afterlife with him.

This practice is common across cultures and time. People so dearly want to cling to their wealth that they will do anything to take it with them. But unfortunately, you cannot take a physical item to a metaphysical dimension.

While I use this analogy in a tongue-in-cheek manner, I think it makes an interesting point about Bitcoin's metaphysical nature based upon math: BTC is the only money ever that you can take to Heaven with you. This is assuming that mathematics still exist in Heaven (and why wouldn't they? Math is metaphysical and therefore could exist in a metaphysical dimension). If mathematics exist in Heaven, then cryptography does as well. And if cryptography exists there, then the blockchain can as well. Just make sure to remember your seed phrase. ;)

Everything we just covered makes a case for the demand, utility and why someone would also be incentivized to hold BTC. As the world's fastest growing technology, it seems like the writing is on the wall for tremendous amounts of value to be stored in BTC.

One of the common misconceptions about something's value is that it only needs utility. But let me prove this point moot. US dollars are quite possibly the most widely used thing in the entire world. Billions of people use the dollar every day. That's a lot of utility. But the fact of the matter is that the wealthy, aside from using dollars to transmit value or engage in commerce, choose to hold as few dollars as possible. Why?

Because although they are widely used, they are pretty much the only asset guaranteed to lose value every day, month, and year. Therefore, utility does not solely equate to inherent value. Value occurs at the crossroads of utility and the desire for people to hold that asset (demand). Bitcoin fits this definition quite well.

Some individuals will get caught up on the idea of whether or not Bitcoin has inherent value. Yes, it does. Inherent value simply means you can use it for something. Water has inherent value because you can drink it. Gold has inherent value because you can make electronic components with it. Sand has inherent value because you can make glass from it. Bitcoin has inherent value because you can use it to transmit value securely and uncensored with a thorough record, to anyone in the world at any time. Having an inherent value is quite a low bar. What people really want to know is if something has market value.

Emphatically, Bitcoin has both.

Chapter Eleven:

What are the Limitations of Bitcoin?

“I think there is a world market for maybe five computers.”

- Thomas Watson,
President of IBM, 1943

History shows us, like the above quote, that sometimes even the brightest minds are sometimes unable to see past a technology’s current limitations. In this chapter we will analyze some of the current limitations of Bitcoin so we can have a fuller understanding of where the tech currently sits, so we can look for solutions going forward.

There is a desired trinity in the perfect Blockchain: Speed, Security, Decentralization. There currently isn’t a single blockchain in existence that has mastered these three qualities, even Bitcoin. Of the 10,000+ blockchains in existence, only a minority of them have even one of these qualities. Bitcoin is in a league of its own because it is the only blockchain in existence that impressively has two of these qualities: Security and Decentralization.

Many crypto projects boast tremendous speed also known as *throughput* on their network. What they will not tell you is that the reason they can get to such great speeds is because they do not have robust security and they are very centralized. For comparison's sake in the current system, the Visa network is very fast (1,700 transactions per second with a stated capability of processing as many as 50,000 tps) and Visa is even quite secure, but they also lack the quality that makes

blockchain so revolutionary: decentralization. Visa makes their own rules and participants must abide by them.

As proponents of a new technology, it is important that we are also honest about its shortcomings. The internet was slow and difficult to use in the beginning, but as more users came and more focus was put on improving the network, innovations like the Netscape Browser made using the internet accessible to everyone, rather than only those with computer science degrees. The concept of YouTube - streaming high-quality video over the internet was an absolute impossibility in the 90s because it could take 60 seconds or more to download even a single low-resolution picture. But the technology moved forward and improvements to the network along with innovative second layer solutions brought the internet out of the dark ages and made it so accessible that grandma uses it without even knowing that the internet is how she's watching Downton Abbey on Netflix.

Speed

On the Bitcoin network, the average confirmation time for a BTC payment is about 10 minutes. And by confirmation, it means that is when the transaction has been input to the blockchain and has been made permanent and immutable.

However, transaction times can vary wildly. You can see a payment come through in seconds. At that point it has been broadcast to the network but hasn't been set in stone. Speed can also be affected by other factors such as the overall network activity and transaction fees. If the Bitcoin network is congested, there will be a backlog of transactions in the mempool - a "pool" of transactions waiting to be processed. This would result in users likely bidding higher fees (remember, the fees are bid by the person sending the transaction, not the miners) to get transactions to go through faster. This occurred in April 2021, where average Bitcoin transaction fees reached almost \$60, regardless of the amount being sent - more on that in a moment.

This is one of the biggest points that skeptics like to point out. If you watch a CNBC segment with an old school investor type that dislikes Bitcoin, you'll see him or her make some variation of the

argument, “How could I ever use BTC at Starbucks when it takes 10 minutes to process? My coffee will be cold by the time I pay.” He or she will usually get a cheap laugh at their overused quip. However, there is a level of truth to this. The base layer of the Bitcoin network trades off speed to be highly secure and decentralized.

Bitcoin didn’t start out as decentralized or very secure, but over its first 13 years in existence it has become a global network with over one hundred million users and nodes - meaning that instead of being able to flip a switch to turn off the network, you would need to flip millions of switches off to shut the network down. That is something no entity or government (even a collection of governments) could do. The Bitcoin network is the most resilient and secure computing network in the history of the world, but unfortunately, part of that security is derived from its slow speed, block times, and the Proof of Work algorithm.

Scalability

As stated before, Visa works well as a global payment system because although it typically processes about 1,700 transactions per second, it can scale up to 50,000tps. Bitcoin can process 7tps. Nope, not 700 or 7,000... 7. While Bitcoin can scale in many meaningful ways such as ease of access to the network to anyone with an internet connection, and the fact that anyone in the world can download a Bitcoin wallet for free, the fact that it’s base protocol is stuck at 7tps is massively prohibitive for it to be used by merchants and individuals all over the world.

One of the attempted solutions to this problem was the catalyst for something known as The BlockSize Wars in 2017. Each block of the Bitcoin blockchain can hold up to 1MB of information. This means that the average block has between 1,500 and 3,000 transactions on it. The Block Size Wars started from a community disagreement regarding ways in which to scale the blockchain. One faction wanted to keep it at 1MB while another faction wanted to increase the block size to 32MB, essentially making it 32X faster. This sounds like a good solution, but the unfortunate side effect is that it would make running a Bitcoin node (storing the entire history of the blockchain) difficult or even impossible

for the average user because it would require nodes to store much more information. Small computers and devices would be prohibited from participating. This goes against the Bitcoin ethos.

A larger block size would mean that only those with larger computer systems could run Bitcoin nodes and thus it would hurt Bitcoin's decentralization. The result of this dispute was a fork of Bitcoin that saw the emergence of Bitcoin Cash (a version of Bitcoin with larger 32MB blocks). Bitcoin Cash was forked again in 2018 creating another chain called Bitcoin SV. These chains have mostly fallen into irrelevance and the Bitcoin ethos of decentralization over speed apparently won out in the free market. The consequence of this is that we remain with a slow protocol that currently lacks scalability at its base layer.

Cost

As the network usage grows, fees grow. While one of Bitcoin's major selling points is banking the unbanked (presumably those with very little wealth), how can we expect the network to scale if the transaction fee to buy something for \$5 is an additional \$10? That simply cannot work.

Volatility

In terms of US dollars, BTC is quite volatile. It is typical for the price to vary by several percentage points on any given day, and a 10 percent drop or increase in a single day is not uncommon. BTC has had a dozen large corrections of 50 percent. While this can be scary with your investment, this is a common phenomenon with new assets.

Volatility can be viewed as good or bad. Volatility over a short period of time can create fear and uncertainty and causes concern for accepting BTC as payment. Afterall, who wants to sell a product only to be unsure as to whether the funds they received will be 10 percent more or less valuable by tomorrow - that's a difficult way to run a business. In the conclusion of this section, we will discuss the positive side of volatility.

There are plenty of news headlines that cause hesitancy about accepting BTC as a payment such as the story of NFL player Odell

Beckham Jr. In 2021 he agreed to take \$750,000 of his salary in BTC. At the time, BTC was valued at \$64,293. By January of 2022 BTC had dropped to \$35,400 - making the value of his contract only \$412,953. As any investor knows, he will only take a loss if he decides to sell, so these headlines are a bit misleading and could quickly be invalidated if the price were to move back up, as it historically does (and as I suspect it will have done by the time you read this book).

The Solution

While we can find horror stories of people that have made poor investments in BTC and have been hurt by the volatility, the interesting thing about BTC is that its volatility over a longer period of time has been *exponential* to the upside. BTC has been the best performing asset of the last one year, four years, and ten years - a nice consolation prize for those willing to withstand short term price fluctuations. A \$100 investment in BTC ten years ago would currently be worth \$260,223 today. If Odell Beckham was paid in BTC for his \$750,000 salary ten years ago rather than in 2021, instead of being worth \$412,953, it would be worth \$1,951,672,862 (yup, that's almost two billion dollars!). Time scale makes a tremendous difference.

This does not change the fact that BTC as a day-to-day currency is a difficult proposition. Currently, BTC is an excellent store of value - like gold 2.0. It's actually far superior to gold in terms of performance and limited supply. It is also far superior to holding USD as a store of value since USD is designed to lose seven percent of its value every year. While BTC's price fluctuations are currently a deterrent against it being used in daily commerce, these price fluctuations over any four-year period have returned wealth transforming growth.

As we discussed earlier, BTC can already be used efficiently in commerce when consumers spend their BTC and an app like Strike instantly turns it into USD for the merchant. This is already a solution that is in place and is becoming more widely adopted. In terms of BTC payments being made and received strictly in BTC, we are still a way off.

Volatility is inherent to emerging assets. Amazon stock was terribly volatile in the early years but has dramatically stabilized after

being in business for over two decades. Bitcoin is young and I expect that after some more exponential growth in price, BTC will eventually stabilize, making it more useful as a daily currency.

No matter how secure and decentralized the network, having slow transaction speeds, high fees, and the inability to work at scale is a problem for everyday commerce. So, to put it bluntly, the solution for speed, scale, and cost problems are being remedied by 2nd layer solutions. This is where protocols like The Liquid Network (a Bitcoin sidechain created by Blocksteam) and the Bitcoin Lightning Network (LN) come into play. Without getting into the technical side of how Liquid and the Lightning networks function, we will mostly focus on the LN here as it has quickly become the most adopted Bitcoin layer two solution.

In its simplest form, LN works like someone running a tab in a bar. Instead of paying for each round, they just close out their tab at the end of the night. Batches of thousands or even millions of transactions can be processed instantly and then later settled with finality on the actual Bitcoin blockchain. So Bitcoin's 7tps can quickly turn into 100,000tps or even 1,000,000tps (multiples of what even a centralized payment system like Visa can perform).

At the time of writing, the Bitcoin Lightning Network was recently rolled out across El Salvador to be used on a national scale. A few weeks after the news of El Salvador, Twitter announced that Bitcoin tips could be sent via tweets using LN - making Twitter the world's farthest-reaching payments network. Anywhere in the world with an internet connection can now receive instant, near free payments.

Perhaps one of the most exciting developments flying under the radar in terms of scale for Bitcoin is Cash App's recent announcement that they have integrated the LN API (application programming interface) into its app. This means that Cash App users can instantaneously send BTC or even USD using Bitcoin as the payment rail to any other wallet in the world that also uses LN.

Why is this such monumental progress in the payments industry? Think about it like this: can you send money from Venmo to PayPal? Nope, and they are sister companies. Can you send money from Wells Fargo to PayPal? Kind of... through an ACH payment that typically

takes 48 hours to process. Can you fund your E*Trade account from your Venmo account? Nope.

This is what makes Cash App's LN integration so important: any wallet, app or device that also integrates the LN API will be interoperable with any other wallet. This means you could send money from the Cash App to PayPal and then fund your investment account and purchase stocks, all with just a few clicks within your app. This realization is what has been making the CEOs of legacy payment systems lose sleep at night.

So, while speed, cost and scalability have been the biggest arguments against Bitcoin's adoption in the past, it appears that these points are being invalidated as I write.

Chapter Twelve: *The Capitalists and the Communists Will Both be Satisfied*

“After the turn of the millennium, much of the world’s commerce will migrate into the new realm of cyberspace, a region where governments will have no more dominion than they exercise over the bottom of the sea or the outer planets. In cyberspace, the threats of physical violence that have been the alpha and omega of politics since time immemorial will vanish. In cyberspace, the meek and mighty will meet on equal terms.”

- *The Sovereign Individual*,
1997

This may be one of the more controversial chapters in this book. I have made many political claims throughout this book, but perhaps no such divide is more of a hot button than that of the capitalists and the communists. It is important to define what I mean by these terms. Capitalism and Communism have both genuine and corrupted forms. I do

not think Crony Capitalists (those that use their wealth and power to bend the system to favor them even more greatly) or devout students of Karl Marx (those that hold to the core values of revolution and the establishment of a government ruling class) will be satisfied by Bitcoin and the coming decentralized revolution. Herein, I will refer to the purveyors of corrupted capitalism as Corporatists and devout Communists as Marxists.

You may notice a similar tone between what I have written throughout this book and the common language used by communists in contemporary American politics: terms like “systemic oppression”. We both see the powerful systems that oppress citizens. We can find common ground if we find a common solution to our common problems.

In fact, Marxists and Corporatists will fight tooth and nail to prevent Bitcoin’s acceptance. Bitcoin disrupts centralized power structures. Marxists and Corporatists agree that power should be centralized. They are also in agreement in their love of inflation because of its *intended* consequence of being a hidden tax on the population. The loss of value in a currency is one of the most powerful tools of these groups, because it allows them to widen the wealth gap between themselves and the rest of the population. Keeping the population poor ensures they are dependent upon the wealthy and powerful.

The Capitalists I’m referring to in this chapter’s title are the genuine capitalists - those that believe in equal opportunity through free markets. I call them the Average Joe Capitalists. The Communists I’m referring to are those that may not be avid readers of Karl Marx but see huge concentrations of wealth in some groups and destitute poverty in other groups because the rich use their wealth and power to bend the system to their will, and they, too, want equality and equal opportunity for all. I refer to them as Average Joe Communists. These two types of people are typically not the political elite. They are regular people that gravitate to one end of the spectrum or another for various reasons. Maybe it’s the culture they were brought up in. Maybe they had an influential teacher that helped to shape their worldview.

I believe that Average Joe Capitalist and Average Joe Communist are not all that far apart. If you sat them both down in a room and explained the merits of an open, decentralized, fair, and balanced

monetary system, and an economic structure where everything from medical research to voting systems were open and transparent, both people would probably be in agreement. If you explained that anyone can have access to financial services and the broader economy, they would agree. If you explained that with almost any amount of money, an individual could buy into a DAO and instantly become an investor in wealth building assets such as real estate or a company startup, both individuals would be in agreement.

If you asked these two individuals if you think that their monetary system should have a hidden tax (inflation) on all citizens, one that especially impacts the middle and lower classes (or, as Marxists call it: the Proletariat and the Bourgeois), both of these people would emphatically say no. They would be in total agreement. If you asked these two people whether a small country being invaded by a much larger and more powerful country should be able to get instantly settled donations from foreign citizens across the globe to protect their homeland, both the Capitalist and the Communist would agree.

The problem for Average Joe Capitalist is that, in our current context, he is fooled into believing that to support Capitalism, he must support what we have now: Crony Capitalism. Genuine Capitalism is the belief that the government should be totally hands off in the markets and that markets have invisible forces that guide them. The genuine Capitalist believes in fairness and competition. Corporatists do not.

Corporatists are Capitalist in name only because yes, while they do make their business from allocations of their capital, they use their massive wealth and influence to lobby the government to intervene in markets. This limits competition and fairness. They lobby for regulation on their own industry (which seems counter-intuitive), but by doing so, they create incredibly high barriers to entry in their industry so the little guy has a much harder time breaking in, if he ever can. This limits competition. They would say they are for limited government, but in practice, they push for concentration of power in the government like the Marxists. They use their influence over government power to help their business maintain maximum profits.

“Competition and low barriers to entry are essential for prices to be fair.”

- Adam Smith,
The Wealth of Nations, 1776

Average Joe Capitalist goes on supporting the broader umbrella of Capitalism, but much of what he is supporting is this corrupted version that goes against his actual beliefs. He's roped into it because of clever political framing. Average Joe Capitalist just wants a level playing field, as does his counterpart, Average Joe Communist.

Average Joe Communist finds himself in a similar circumstance as Average Joe Capitalist: supporting a version of Communism with which he does not entirely agree. Average Joe Communist wants equal opportunities in the economy as well. He favors laws that ensure equal rights, but he is not ok with top-down authoritarian Communist rule because he knows it ultimately leads to oppression and limits on equality.

Staunch Progressives have long railed against corporations, but there's very little difference between government and these corporations. Corrupted Capitalism has top-down rule in the same way Communism has top-down rule. Average Joe Communist understands that government has the additional power of legal violence to enforce what it wants, which is a far more terrifying prospect than corrupt Corporatists. It's a strange paradox that those who traditionally distrust corporations, have a lot of faith in government. The world's wealthiest man, Elon Musk, had this to say:

“Government is essentially the biggest corporation with a monopoly on violence.”

The definition of wealthy and poor has changed over the years. As I have mentioned, I call myself a Bleeding Heart Capitalist (BHC). One of my favorite questions to ask my liberal friends who believe in communist ideologies is, “Would you rather be poor today or the king from 200 years ago?”

At first, this sounds like a very dumb question. Of course, you would want to be the king, right? I wouldn't. I'd rather be poor today. Yes, the king would have some cool power but that's not what I'm talking about. I'm talking about your daily comforts and standard of living.

The king from 200 years ago did not have access to the world's information in the blink of an eye (via the internet). He did not have a refrigerator or a freezer. He didn't have hot and cold water. He didn't have plumbing. He didn't have an AC or a heater. He didn't have video games or other electronic entertainment. He didn't have dozens of restaurants, many of which were open 24 hours a day. In fact, even as king, his menu items would be fairly limited. He didn't have access to antibiotics if he got a life-threatening bacterial infection. He didn't have toilet paper. His drinking water was never perfectly clear and it was always room temperature. He didn't have a car. He didn't have electric lighting. His life expectancy was about 50 to 60 years old.

When considering these things, without a doubt, I would rather be poor today than be king 200 years ago. This begs the question, how does a poor person today have a better standard of living than the world's wealthiest person from 200 years ago? This is because over the last 200 years, markets that allowed businesses to compete have enabled industry and innovation to flourish. Everyone benefits from this. Things get much better for everyone when incentives align in such a way that a person who creates something that benefits society gets some upside for themselves as well.

I even like to take this thought experiment one step further. I'll ask my friend, "Have you ever considered how the average American today has the luxuries of a millionaire from the 1980s?" I'm not talking about 200 years ago. I'm talking about less than 40 years ago. They'll usually respond with something like "Psshhh, yeah right!" as they roll their eyes.

I'll then lay out the similar luxuries a millionaire from 35 years ago had to the average American today. The average American has a personal chef that will serve them any type of food they want at any hour (DoorDash). They have a personal driver (Uber). They have a cell phone (for those that don't know, a 1980s cell phone was a wealth status

symbol). They have a personal stockbroker (Robinhood). They have a movie collection with thousands of movies (Netflix). They have a massive music collection (Spotify). They have a personal shopper (Instacart).

Again, why, in only 35 years can we go from these luxuries being limited to the ultra-wealthy to now being available to anyone at any time? This is because Capitalism fosters innovation and drives growth. The saying goes, “A rising tide lifts all boats.” This is certainly an apt saying to describe the phenomenon of increasing access to goods and services to all. Karl Marx himself even admitted that Capitalism was a driver of innovation.

“Capital is money, capital is commodities. By virtue of it being value, it has acquired the occult ability to add value to itself. It brings forth living offspring, or, at the least, lays golden eggs.”

Marx’s chief claim against capitalism was that it causes boom and bust cycles. This is true in Crony Capitalism. It’s actually the intervention of government that creates monopolies and regulatory capture (collusion between big business and the government agencies that are supposed to regulate them). Competition is required for true capitalism, and what I believe Marx identified was that Capitalism can be corrupted and that the mega powerful can squash competition. Marx’s solution to this was to create a top-down control so that corporations couldn’t do this, because he had no other option. I think it’s possible that Marx could have seen blockchains, rather than the government, as a viable option for enforcing fairness.

I believe Marx’s shortsightedness was that he underestimated the fact that centrally planned Communist governments would have the same type of corrupt, power hungry individuals in charge, and they would essentially do the same things that the mega powerful Capitalists did.

So, if Capitalism and Communism can be corrupted because they ultimately are only as good as the people who are in power, what is the solution? Simple. The solution is a programmatic, rules based-system

that is not subject to human fallibility. The rules are established ahead of time and those who like those rules will choose to live under that system. They do not have to worry that the system will be corrupted by malevolent forces because their governance is performed by decentralized and transparent systems.

Imagine if we could program the US Constitution and our laws into smart contracts. We wouldn't have to rely on partisan Supreme Court Justices (they aren't supposed to be partisan, but we all know they are) to rule on the constitution with all their biases and imperfections baked into the decision. Individual rights would be protected in a fair and just manner. A corporation could not wield influence over the set of rules. Nefarious politicians would be forced to govern in an open and transparent manner.

This type of system ensures equal rights, equal opportunities, and fair competition. The Capitalist likes that. The Communist likes that too.

A fundamental tenet of Communism is that workers get the fruits of their labor. Communists do not like it when laborers do all the work, but the owner of the company gets all the profits. In Bitcoin, there is no owner. Miners perform all the work to maintain the network and they receive all the mining rewards for doing so. This type of incentive structure can be applied across all sorts of industries.

Li Jin, a self-proclaimed student of Marx, publicly stated that this form of corporate governance was the "next step forward in the labor movement."

The type of corporate governance he was referring to is a DAO (a Decentralized Autonomous Organization - an organization structure where token holders make all the decisions). DAO's are the ultimate creator of the level playing field in terms of corporate ownership. Owning an NFL football team is resigned to only the ultra-wealthy, correct? Not any longer. There are currently DAO's being created where individuals with virtually any amount of money can buy in and own a piece of a professional sports franchise. A poor single mother could scrape together even a modest sum of money and create a second stream of income through a DAO - she could even put on her resume that she owns the Denver Broncos!

Decentralized monetary and corporate systems will be the ultimate drivers of equality through the coming decades.

The latest and most genuine version of Capitalism, Bleeding Heart Capitalism, is all about aligning incentives so that in an individual's pursuit of wealth and personal betterment, they create wealth and opportunity for others. Blockchain governance is a fundamental tool in this.

I love Brazilian Jiu Jitsu. I've trained for the better part of a decade, typically 5-6 days per week. I am a part of a world renowned team called Checkmat. In 2021, Checkmat won the BJJ team world championship. I have visited other, less renowned gyms before, as well. Seeing the ecosystem within a thriving BJJ school vs that of a lower quality school, has helped mold this concept of Bleeding Heart Capitalism for me.

The difference I noticed is in the attitude of the black belts. In the rather unremarkable BJJ schools, the black belts and other more advanced belts (purple and brown) look at the lower belts as an opportunity to beat up on someone. This might be fun, but it does not help the lower belt, and it does not further increase the skill of the black belt since it's such a low level of competition for them. Their lower belts never improve because they are always being crushed, and the upper belts do not improve because they never face stiff competition.

In the thriving gyms you will notice that the black belts are very gentle with the lower belts. They roll (spar) at, or just barely above the level of their students. This might not stroke the ego of the black belt, but it helps their students flourish and develop proficient skill.

How does this apply to Bleeding Heart Capitalism? The black belt that focuses on bettering others will inevitably see his own skill grow because his students will develop and eventually become proficient enough to challenge the black belt. The presence of stiff competition makes everyone better, including the black belt. On the other end of the spectrum, the black belt that crushes his students to suit his own ego will see his skills stagnate. Everyone is worse off in a gym without good competition.

The point here is that the black belt who serves himself the best is the one that helps others along the way. This same principle is true in markets. A Bleeding Heart Capitalist who recognizes the fact that if she fosters her community to grow, flourish, and become wealthy, she will simultaneously be fostering a customer base that will ensure the long term success of her business. If you own a business, you should want everyone around you to be rich and thriving, because this means there will be more wealthy people around you to buy your stuff.

In our modern culture we hear the terms equity and equality thrown around. Most people use them interchangeably, but they are two very different concepts. Equality means equal opportunity. Equity means equal outcomes. For example, equality would mean that two different students from two very different backgrounds, with similar grades, both get an opportunity to go to an Ivy League University. From there, they will either succeed or fail based upon their individual merit. Equity would mean that not only would both students be able to get into that Ivy League University, but regardless of one student failing all their classes and the other student getting all A's, both would get to graduate with honors. Equality and equity are very different.

We can never have wealth equity. It is just simply impossible. The idea of redistributing wealth equally to all citizens seems like a benevolent idea, but it is fallacious. This has been studied for decades.

"It is to be regretted that the rich and powerful too often bend the acts of government to their selfish purposes. Distinctions in society will always exist under every just government. Equality of talents, of education, or of wealth cannot be produced by human institutions. In the full enjoyment of the gifts of Heaven and the fruits of superior industry, economy, and virtue, every man is equally entitled to protection by law; but when the laws undertake to add to these natural and just advantages artificial distinctions, to grant titles, gratuities, and exclusive privileges, to make the rich richer and the potent more powerful, the humble members of society—the farmers, mechanics, and laborers—who have neither the time nor the means of securing

like favors to themselves, have a right to complain of the injustice of their Government.”

- Andrew Jackson

In my high school economics class, the teacher gave each student 100 “Econ Bucks” at the beginning of the semester. You could trade them with your classmates as you chose. You could pay a classmate to help you with an assignment. You could even pay the teacher to let you leave class five minutes early on Fridays. What happened during our semester was what the teacher said happened in every one of his past semesters with this process. At the end of the semester some students had none left, a lot of students had some but not much, and the one or two enterprising students had about 80 percent of the currency. They were the ones that were willing to delay gratification and had found creative ways to offer value to their classmates that were willing to part ways with their currency.

We see this same type of phenomenon in economies. It's important to consider that people have different goals and desires. Not everyone wants to be rich. Some people want to be rich, but they lack the discipline to maintain wealth. Others are dealt a bad hand.

If you want equity, then you must occasionally redistribute wealth, but the same wealth concentrations will eventually happen again. The Bleeding Heart Capitalist knows that his wealth isn't in the currency. Hoarding dollars will never make him truly wealthy. The best path of maximum self-interest is if he can invest some of his currency into the labor of the “have none” class, then he will be able to create assets or wealth generating enterprises that benefit him and tangentially turn a “have none” into a “have some”. In a fair and balanced system, that new “have some” individual can copy exactly what the wealthy individual just did - turn around and move his wealth out of currency and into wealth generating assets. A fair system levels the playing field so that any individual who so desires can use this strategy to break the cycle of generational poverty.

“It is not from the benevolence of the butcher, the brewer, or the baker that we can expect our dinner, but from their regard to their own self interest.”

- Adam Smith,
The Wealth of Nations, 1776

Even with a fair system there will still be “have noes”. The poor will always be with us to some degree. So charitable giving is an important aspect of Bleeding Heart Capitalism as well. But how do we incentivize a wealthy person to donate their money to those who need it? We appeal to their generosity and maybe even their vanity and give them economic incentives to do so.

NFT’s (one of a kind digital tokens) may be one of the building blocks of this movement. NFT’s can be created to commemorate charitable giving like donations to catastrophic events. The businesses or individuals that donate would receive rare tokens that represent their generosity. They can brandish these items on their social media accounts, websites, or even display them as physical art. NFT’s even have monetary value. In 2020, Jack Dorsey (founder of Twitter) sold an NFT of the first tweet ever for \$2M. The tweet was not particularly compelling. Dorsey simply tweeted, “just setting up my twitter.” If a rather pointless tweet can have value, being able to display art that represents one’s participation in ending regional hunger in Africa surely has value as well.

From DAO’s to NFT’s to constitutions built on smart contracts, blockchain technology has the fundamental components to develop a social structure that is genuinely fair and provides a level playing field for all people. I believe that this appeals to Average Joe Capitalist as well as Average Joe Communist. Their corrupt forms will not like this, but the vast majority of people in the middle absolutely will.

I have repeatedly referred to myself as a Bleeding Heart Capitalist throughout this book. I am fond of this term because as a young boy I remember my father, who was a staunch Republican, making fun of our Democrat neighbor for being a “bleeding heart

“liberal”. I thought that sounded like a strange thing to say, especially because the thing he was making fun of her for was a policy that was intended to help poor people. He listed all the rational reasons as to why a government program wouldn’t fix that problem and what he said made sense.

As I grew older and I began to further study the Bible (the foundation of my Christian faith), as well as economics, I found myself having a heart for helping people. I came to the conclusion that Capitalism and free markets were more efficient tools for helping people than the government. However, the capitalism I often saw was a pretty heartless form. So, I became a proponent of *Bleeding Heart Capitalism* - an economic system that recognizes both the need to help others and the fact that capitalism is the most efficient economic force for doing so. I believe this economic system with Bitcoin as its substrate, can satisfy both the Capitalists and the Communists.

I referenced this quote in the introduction, but it bears repeating here. I believe that Fuller’s quote below describes what’s at stake with regard to our decentralized future. Perhaps it’s an end to the fiery partisan divides that have driven wedges between friends, families, churches, and communities.

“*You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.*”

- R. Buckminster Fuller,
Architect, Systems Theorist, and Futurist

Chapter Thirteen:

Short Answers to Common Questions

#1 Why won't Bitcoin be like Myspace or Yahoo?

Answer: There are two points to consider here. First, Bitcoin isn't a company. Bitcoin is a protocol. So instead of thinking of Bitcoin as a Myspace type company that could eventually be outcompeted by a competitor (Facebook) with a better user experience, more capital, or a viral marketing campaign, Bitcoin should instead be thought of as a protocol like the protocols that run the internet (TCP/IP, SMTP, HTTP, etc.).

So, where there are plenty of examples of first mover companies that were usurped by newer and better rivals, there aren't these same examples when it comes to protocols. The main reason being that protocols are open-source, and everyone can use them. Therefore, everyone can benefit from them. Companies can be thought of as "closed-source". When Facebook was starting up, there was no way for them to piggy-back on Myspace by building a Facebook page on the Myspace website. The only viable option for Facebook was to build a different website and ultimately try to take users from Myspace.

With Bitcoin as a protocol, the companies that want to interact with it can benefit by integrating with it and building on top of it. For example, Cash App is a payment app, but they have integrated the Bitcoin Lightning Network into their functionality. Doing so instantly scaled their app to be able to interoperate with dozens of various Bitcoin wallet apps, and other payment apps using the Bitcoin LN.

As I briefly mentioned earlier, in 2021, Twitter also integrated the Bitcoin LN into its system - instantly turning Twitter into one of the world's largest money remittance networks with over 260M users. Twitter, a social media platform became a worldwide player in a new space (payments) with one integration. Discover and Visa cannot even send funds directly from one app to the other, but by using Bitcoin as a protocol, Twitter is capable of sending money to 260M of their own users, any of the 30M monthly Cash App users, or any of the other 100M+ Bitcoin wallet users.

Key Point: Protocols are different from companies.

Secondly, if the skeptic really just wants to make the comparison of Bitcoin as a first mover company (like Myspace or Yahoo) then I will indulge them for a moment, even if it's an inaccurate comparison. *No company in history has been usurped after reaching a \$100B market capitalization.* Bitcoin has already surpassed a value worth over 10x that amount. Myspace's market cap was less than \$12B at the time it was surpassed by Facebook, and Yahoo was valued at less than \$5B when Google became the dominant search engine. Twelve billion and five billion are large sums, but they are a far cry from \$100B, and most certainly from the \$1T market cap that Bitcoin reached in only 12 years.

If Bitcoin were a company, there would be no historical precedent for it to be surpassed by a new entrant into the market.

Lastly, while Bitcoin is the first crypto currency, as we know them today, it isn't the first digital currency that was ever created. Hash Cash, eGold, eCash, and others attempted to solve the digital currency problem but were unable to. Additionally, I have made the case throughout this book that fiat currencies are the "old tech" that Bitcoin will disrupt. Compared to past digital currencies and fiat currencies, Bitcoin can be thought of more as the Google disrupting Yahoo rather than the other way around.

#2 What is the difference between a coin and a token?

Answer: If you've been in the crypto space for any period of time, you may have heard both the term "coin" as well as "token" thrown around. One may just assume they mean the same thing. Many people do use them interchangeably, but they actually mean different things in a technical sense.

A coin is the digital asset produced by a blockchain. You can think of it like the native asset of the blockchain. Smart Contract blockchains like Ethereum have an ETH coin, but since dApps can be built on top of Ethereum, those dApps can also produce their own digital assets. The digital assets produced by the dApps are called tokens.

You can think of this like a video game arcade. When you walk into the arcade you have dollars. That's the base currency that is accepted everywhere. You can go to the concession stand and buy popcorn or you can walk over to the video game section and exchange your dollars for tokens so you can play the games. The video games are like the dApps, you use your tokens to play them.

Just like you would exchange dollars (coins) for game tokens, on Ethereum, you need to exchange your ETH for that dApp's token in order to use that dApp's service or to play its game. In practice, this is a seamless transition.

Currently, Bitcoin's blockchain and others like XRP and Litecoin only have coins. They may have robust smart contract capabilities someday and then have tokens, but currently, they do not. These blockchains intend to function as money/currency so they do not really concern themselves with dApps yet. Smart Contract platforms like Ethereum, Solana, and Cardano, have both coins and tokens because they do not aim to function as payment protocols, but rather, as the building blocks for more open-ended infrastructure.

#3 Is Bitcoin a Ponzi Scheme?

Answer: I have noticed that most skeptics who lob this accusation at Bitcoin do not specifically understand what a Ponzi Scheme is. The definition of a Ponzi Scheme is that it is a fraudulent enterprise that promises quick returns to investors, but rather than performing a business or a service, returns are only paid out to older investors by incoming funds from new investors. In essence, the first round of investors get paid out by the funds from second round investors. The second gets paid out by the third and so on. Eventually, there will be no new investors and someone will be left holding the bag.

In a Ponzi Scheme, investors are lied to about how profits are made. Charles Ponzi (the man after whom the scheme is named) did not have a legitimate business, but because he knew no one would invest in an obvious pyramid structure investment, he told them he was buying and selling postage stamps. This was a lie, and the only funds coming into or going out of the company was capital from investors.

The early investors in Apple sold their shares at a profit to later investors in Apple. Why isn't that considered a Ponzi Scheme? Because the later investors got to hold Apple stock, which is a share of a company that continued to have value because of the function it served as a business. The value proposition of holding stock was open and transparent to both early investors and prospective investors. As a publicly traded company, Apple must provide documents about its finances and business operations to the public every quarter. Everyone had informed consent before they entered into the investment.

Bitcoin is not a Ponzi Scheme for the same reason that Apple is not a Ponzi Scheme. Both early and late investors get to hold the digital asset for which they purchased. The value of it may go up and down, but the intended purpose of Bitcoin is to function as a monetary network. Both the early investor and the later investor can use their BTC for its intended purpose to send money all around the world. The promise of Bitcoin is not to get rich. The promise of Bitcoin is to be able to remit value without censorship using an immutable and transparent ledger.

In the same way that Apple can be audited by prospective investors, Bitcoin can be audited by anyone at any time by looking at the blockchain explorer. In fact, the Bitcoin blockchain audits itself every ten minutes by every node on the network. It's the most audited entity or network in the history of the world. Ponzi Schemes are opaque. Bitcoin is the most transparent entity in the history of the world.

#4 Will Bitcoin be like Tulip Mania?

Answer: For those not familiar with Tulip Mania, it was a Dutch fad in 1636. Tulips were a new type of flower that the Dutch hadn't seen before. They quickly became a status symbol of wealth and sophistication prompting demand to go through the roof. At their peak, a single tulip sold for as much as 10,000 Guilders (Dutch dollars) - the equivalent cost of a mansion – in today's dollars it would be about \$1.5M.

How did Tulip Mania crash? Well, in 1637, the next harvest year, everyone had had the same idea - plant your tulip bulbs from last year and grow more tulips! We all know what happens when an exclusive item that represents wealth and class becomes common; it no longer represents wealth and class. The value of tulips crashed in the early days after the harvesting of new tulips. Instead of one tulip costing a year's salary or even as much as a mansion, in 1637 an entire cartload of tulips was worth only a few dollars. In some cases, people wouldn't even take them for free.

The Tulip Mania and Ponzi Scheme comparisons seem to be made by the unenlightened or uninformed. They sound clever or witty, but they ultimately illustrate the person's ignorance of the principles of Bitcoin. That's ok though, we all once shared that ignorance. It's the job of the Bitcoin Evangelist to shed a little light on these misinformed perspectives.

Comparing BTC to Tulip Mania is perhaps the most egregious offender in terms of poor arguments because it's not only inaccurate, but it is also the *exact opposite* of how things are. The Tulip Mania bubble burst when the supply of tulips was inflated. Humans saw an opportunity

to produce more, and in turn created a far greater quantity of tulips than there was demand for. Tulips are much more akin to fiat currency than hard money like gold or BTC. Fiat can be produced at will. Tulips can be produced at will. BTC cannot be produced at will.

The follow up argument from the skeptic would be, “Well, maybe you can’t create more BTC at will, but you can create a brand-new crypto currency at will. After all, aren’t there like 10,000 different cryptos?” Yes, there are over 10,000 various crypto assets on their own blockchain. This is what happens when you have open-source software; it can be copied. You can even copy Bitcoin’s software right now and start your own Bitcoin 2.0 in a few hours.

Surely, the skeptics must be right then, and this is just like Tulip Mania! False.

How is that false? The answer is simple: network effects, decentralization, and security.

As I just mentioned, you could go start your own Bitcoin 2.0 today. Let’s imagine that you did. We’ll call your coin BTC2. BTC (the original) trades for about \$50,000. Now try and go on the internet and ask people to buy your coin for \$50,000. No one will pay. They likely won’t even pay you twenty dollars. Why does no one want it? Because it’s not BTC, it’s something entirely different. BTC has over 100M people connected to its network, BTC2 has one person connected to it. Furthermore, your network is not very secure, and it is highly centralized. In order to hack BTC2, someone would just need to have more hashpower than your home PC.

Let me illustrate the network effect in another way. English is one of the most widely spoken languages in the world. But you could go and create your own language today. Nothing is stopping you. Unfortunately, when you go to a restaurant and try to order food in your new language, you will soon find yourself frustrated and hungry. You’ll switch back to English for a practical reason: it works, and you want food.

Why is English more valuable than your new language? Because it has a tremendous network effect. It’s a common language that many

people speak. Bitcoin is a common financial protocol language that 100M nodes and a growing number of institutions all over the world speak.

Tulips can be copied (by growing new ones) and the copies have all the qualities of the original. Bitcoin can be copied but the copies do not possess all the qualities of the original.

#5 I heard that the government could confiscate BTC. Is that true?

Answer: This question became most prevalent during the 2022 Canadian trucker Freedom Convoy. After several attempts at crowdfunding to support the protest against Canadian government vaccine mandates had failed, donations began coming in via Bitcoin. The Canadian government enacted the Emergencies Act, which granted authority to the national government to freeze individuals' bank accounts and prosecute anyone who was making donations to the truckers. It was one of the most authoritarian moves seen by a significant western country in a lifetime - and in a post 2020 world that's saying a lot.

Headlines began running on all major news networks and in major publications to the effect of, "*Canadian Government Freezes Bank Accounts and Crypto Wallets Via The Emergencies Act*". Both conservative and liberal media outlets mocked Bitcoiners with accusations such as, "Ha! Look! The one thing that Bitcoiners thought they could do (resist government intervention) has not worked. Bitcoin wallets are being frozen and seized by authorities."

If you still believe there is truth in headlines, then I don't know what to tell you. These headlines were misleading to say the least. What articles and news anchors failed to mention is that only crypto funds held on exchanges like Coinbase, Kraken, Binance, etc. can be frozen. Why? Because they are *centralized* exchanges. In this context they are no different than having your money at the bank. They must register with the government and come under regulation to operate.

What the articles and headlines should have been saying was that non-exchange wallets were immune to this government regulation. In the days after the Emergencies Act was enacted, videos began surfacing on the internet of groups delivering documents to the Canadian truckers with private keys for Bitcoin wallets with thousands of dollars in them so the protests could keep going. These private key deliveries protected both the individuals donating, and the truckers receiving the donations from government overreach.

Non-exchange wallets are just programs that you can download on your computer or device that enable you to hold your BTC. Popular non-exchange wallets include Ledger, Nunchuk, Trezor, Exodus, Electrum, and BlueWallet.

While there are plenty of small-scale similar stories like this from developing nations over the past decade, the Freedom Convoy protest marks the first time Bitcoin was used to protect citizens and civil liberties from a western authoritarian government.

So, the simple answer to this question is that if you keep your BTC on an exchange, then these kinds of confiscations are quite easy. If you keep your BTC in a private wallet that only you have the keys to, then government confiscation is very difficult if not impossible.

#6 Can Bitcoin be banned?

Answer: The next logical question after realizing that BTC cannot be frozen or seized when held in a private wallet is to ask, “Yeah, but can BTC be banned?” Fair question, and the answer is yes. Yes, a government is a sovereign power, and they are free to write pro Bitcoin laws or anti-Bitcoin laws.

I will say this though, If you cannot confiscate something, then how effective is a ban? Not very. For example, China has banned BTC twelve times. Crypto skeptics will point to that and say, “See China hates Bitcoin and therefore they are crushing it.” My response is pretty simple. If banning it is so effective, then why were eleven additional bans made after the first one? Certainly BTC has become less popular in China since

the government crackdowns but it has not eradicated BTC from its borders by any means. Chinese speculative investors have gotten out of the market, but among those who use BTC for its intended purpose, it is alive and well.

#7 How does BTC mining work?

Answer: Bitcoin mining in its entirety can be complicated and require knowledge of various computer science and cryptography terms, but I'm going to give you a basic rundown to help you wrap your mind around the process. First off, it's important to understand why mining even exists. Satoshi Nakamoto came up with mining as a way to incentivize unknown people on the network to validate transactions, make Bitcoin more decentralized, and keep the network safer.

You can't just expect people to volunteer computing power out of the goodness of their heart, so you need to reward them with something. That's why each block that gets validated by miners and added to the blockchain comes with a reward. These miners all run the open-source Bitcoin software that uses what's called a Proof of Work (PoW) algorithm. This ensures that all miners are playing by the same rules. To receive the block reward, they must prove to everyone else on the network that they actually did the work (supplied a bunch of hashpower to the network to keep it safe).

This "work" in the Proof of Work is where many people get confused. Most often you'll hear a talking head say something like, "Crypto mining is essentially solving a highly complex puzzle." The process might be complex, but a puzzle would not be a good way to describe it. A better way to describe it would be as a lottery, or a giant game of "pick a number between one and ten," but with near infinitely greater numbers.

The actual validating of transactions is a very simple process for computers and it doesn't take much computational energy. Where the vast majority of energy is expended is in this lottery. Each ten minutes the Bitcoin algorithm produces a new random number called the nonce. This stands for "number used once". The nonce is like the winning

lottery number, but in this lottery, it is picked at the beginning, and no one knows what it is. Instead of buying lottery tickets, anyone that wants to enter the lottery can just try to guess the nonce. If you guess wrong you can just guess again, and again, and again. The technical term for this guess is called a hash.

The lottery doesn't end until someone guesses the correct number. But this number is so large that it's statistically far more likely for someone with one lottery ticket to win the Mega Millions lottery than for one thousand guesses to win the Bitcoin block reward. Because everyone gets unlimited guesses, this means that the faster the computer you have, the more guesses you'll get. For comparison, the average smartphone can make about 1,500 guesses per second.

Mining has become such a big industry that there are now publicly traded companies that have warehouses full of high-speed computers optimized (called ASICs) to guess the Bitcoin nonce as fast as possible. To say that the race for the nonce is a competitive one would be an understatement. Currently, the hashrate of the Bitcoin network is 248.11 million terahashes per second. Each terahash is one trillion hashes, or guesses. This means that Bitcoin miners have so much computational power that they guess 248 quintillion times *per second!* The nonce is such a large and complex number that it takes, on average, ten minutes for miners to guess the nonce at that hashrate!

Here's the beautiful thing about all that hashpower - it's what is securing the blockchain. And that's, in part, why we can confidently say that Bitcoin is by far the most secure network on the planet.

#8 Isn't Bitcoin Bad for The Environment?

Answer: In a world where the World Economic Forum (WEF) has effectively propagandized their initiatives, most broadly ESG (Environment, Social, Governance), anything that threatens to undermine the status quo will inevitably face backlash. One of the chief accusations from skeptics toward Bitcoin is that it is bad for the environment.

Allow me to give you one such example of the ESG propaganda that is launched against Bitcoin. The proponents of ESG are supporters

of electric vehicle production such as Tesla. And rightfully so. Tesla has created efficient, long-range electric vehicles and continues to push the envelope in research and development. Tesla cars are the epitome of the green movement.

Bitcoin mining hardware emits the exact same amount of carbon as a Tesla car does, zero. Bitcoin mining hardware emits the exact same carbon as your smartphone, your computer, or your TV. None. This confounds those that have perpetuated the propaganda of “Bitcoin mining is bad for the environment”. When you distill it down, what people are really concerned about is what fuel source is providing the electricity for these devices. If you charge your Tesla overnight from an electric source where the electricity is produced by coal, then are you really limiting greenhouse gasses? No.

The same is true for bitcoin mining. If your bitcoin mining hardware is plugged into a source of electricity that was generated by fossil fuels, then your mining operation is leaving a carbon footprint. If your mining hardware is powered by renewable, green energy, then you are having a net neutral impact. According to the Bitcoin Mining Council, across all industries, less than 20% of renewable energy is used.

This means banks, carwashes, grocery stores, fast food restaurants, the Apple Store, and all other companies use less than 20% renewable energy. Because bitcoin miners are financially incentivized to use the cheapest energy source possible, they naturally gravitate toward renewable energy. The bitcoin mining industry uses over 60% renewable energy (over 3x greater than other industries).

Why does the ESG movement rail against Bitcoin if Bitcoin isn’t actually bad for the environment? This quote from Peter Thiel may offer some insight into the answer to that question.

“When you hear ‘ESG’, you should think ‘CCP’ (Chinese Communist Party)”

The accusation against Bitcoin being a “dirty polluter” comes from the energy intensive nature of blockchain mining. Mining does take a considerable amount of power, but it is not for nothing. It serves a purpose - to protect individual sovereignty, freedom, wealth, and to

preserve the world's first ever decentralized monetary system. When you look at what that energy consumption is preserving, then it starts to make clear the motivations of why globalist entities like the WEF, CCP, IMF, or BIS are attempting to stifle Bitcoin. Keep in mind that all this energy consumption is fueled by much cleaner sources than the detractors would like you to think.

Other popular detractors like US Senator Elizabeth Warren or the current US Treasury Secretary Janet Yellen (former Fed Chairwoman) will use inaccurate data to make anti-Bitcoin claims about dirty energy consumption. For example, they will cite the “per transaction energy cost”. But by calculating it this way, it just shows that they do not understand how the network works. Energy costs do not go up with the scale of transactions. The same amount of energy is used by Bitcoin miners if there is only one transaction or 100,000 transactions.

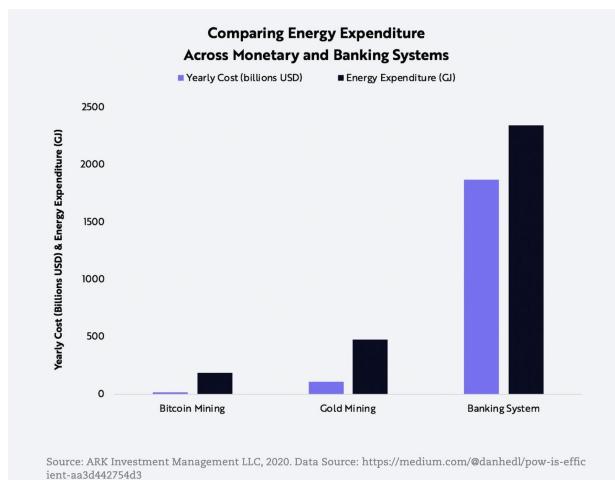
Computational power and energy cost is relative to the security of the network, not the transaction throughput. At the very beginning of Bitcoin there were only a handful of computers running the blockchain. The annual cost of electricity would have been several hundred dollars and less electrical consumption than a typical American home. At that time Bitcoin was capable of the same number of transactions as it is today with its current vastly superior hashrate. If Bitcoin could process 10M more transactions per day, it wouldn't require any additional energy.

Allow me to reiterate, it's important to note that energy consumption by blockchains is what makes it secure, not fast. Processing transactions takes very little computational power. Being the world's most secure computer network takes a lot of power. In a nutshell, anytime you see someone being antagonistic toward Bitcoin and citing per transaction costs of energy, know that they are illustrating their lack of knowledge of how Bitcoin actually works.

Another energy related accusation against mining is that it “uses the same amount of energy as a country”. Understand this, and this is true for all types of headlines and brief, witty-sounding statements on any subject from medicine to politics: many comparisons may sound impactful, or as though they prove some sort of point. But we need to ask ourselves, “What does it really mean?” Saying that Bitcoin uses the equivalent power of a country sounds impactful. We must then ask the

question, “What size country?” If you look further into the claim they will clarify that they mean a *small country*. Even that still sounds impactful so we must ask the next logical question, “How much energy does one of these *small countries* use?”

Let’s put the energy consumption of a small country into perspective. Americans use more electricity in the month of December on Christmas lights than small countries like Uruguay, Ethiopia, and Tanzania use in an entire year⁽⁴²⁾. Furthermore, among similar industries, Bitcoin pales in comparison with regard to energy consumption. Ark Invest performed a study which shows Bitcoin’s energy consumption versus gold mining and the amount of power used by our current banking system (which does use energy on a per transaction basis).



It’s strange that US Senators and the WEF are not publicly denouncing Christmas lights, gold mining, and banking energy consumption. I wonder if that’s just because those things do not challenge the status quo.

There are also regular individuals you will encounter who may parrot these headlines. They may even quote these misinformed Senators as though what they say is gospel. Chris Williamson calls this type of vain and unsophisticated conjecture *mid wittery*. Mid wittery is the phenomenon where a misinformed individual arrogantly makes a statement based upon bad information, but they say it with great

enthusiasm and confidence. It sounds sophisticated, but it's actually quite intellectually shallow. "Bitcoin having high *per transaction* costs" and "using more electricity than a small country" are two examples.

Not only will Bitcoin not be a net *negative* for the environment, I think it will be a net *positive*. In chapter 5 I laid out the case for what I call *Green Bitcoin*. Please feel free to revisit that chapter to fully formulate your thoughts on this question. From my perspective, Bitcoin mining will be the key to making sustainable and renewable energy possible for mass scale.

If we have learned anything about post-2020 culture, it should be that sometimes the accusations made by those in power are not only untrue, but they are often the exact opposite of truth. It may come to pass with Bitcoin that the current upholders of the status quo repeat the talking points of mining being a detriment to the environment, but in the end, it is Bitcoin that drives sustainability to planet Earth.

#9 Why would someone mine BTC when they could just buy it?

Answer: There are several reasons for this. If you have an efficient enough mining operation you can mine BTC far more cheaply than what you can buy it for on the open market. At the time of writing, BTC's spot price is about \$37,200. Efficient miners can mine a BTC for about \$9,000, on average⁽⁴³⁾. They are getting a \$28,200 discount on each coin.

Aside from the profit, an individual may want to mine BTC because they are considered "virgin BTC". This means that the ownership of the coin is completely anonymous. If you bought your BTC from a centralized exchange like Coinbase, you could have a paper trail to your coins. Virgin coins also have the added benefit to the owner of having certainty that their coins were not used in illicit activities.

I personally think this isn't very compelling though. While I do not want crimes to be perpetrated, I don't really care if the coins I hold were previously used for a bad activity. I would have no moral

responsibility for that crime. I've never cared to know if my USD was used in crimes, and I feel the same way about BTC.

#10 What should I do if I can't afford an entire bitcoin?

Answer: Individuals should get away from thinking about needing an entire BTC. If you can make that happen, then great, but for most people the high cost of a single coin seems prohibitive. In the future, holding a single coin will likely have a similar status to someone today who we call a millionaire. You would never quit your job and stop trying to acquire dollars because "being a millionaire is unattainable". But some people give up on accruing smaller amounts of BTC because they are discouraged at the thought of never owning an entire bitcoin.

Rather than thinking about a whole bitcoin, think in terms of Sats - the smallest unit of bitcoin (like a penny to the USD). In Bitcoin circles there is a phrase, "Stack sats and chill." This simply means that the best way to gain exposure to BTC is to buy bits of it at a time. There's a common misconception that one must buy an entire BTC. This isn't true. Accruing small amounts over time is a much more reasonable strategy than taking a drastic measure like mortgaging a home to buy an entire coin.

#11 Who is Satoshi Nakamoto?

Answer: The public does not know who Satoshi Nakamoto is. Perhaps no one outside of Satoshi himself knows who he is. I suspect there's a small group of close contacts who do know his identity. The reality is that Satoshi's identity does not matter. It seems clear that he didn't hide himself because he was scared, but rather, because he cared about the future success of Bitcoin. He even said in forums that critics would be quick to attack Bitcoin over any of Satoshi's personal inadequacies. He

kept his identity hidden so that critics would have to attack Bitcoin based on merit.

There are plenty of fun documentaries on Satoshi's real identity. Check them out if you are really interested in this topic. My personal opinion based upon very limited research on this particular subject (I haven't studied this much because it's largely irrelevant, but human inquisitiveness will naturally prompt some curiosity) is that Satoshi Nakamoto is a man named Adam Back. In 1997, he created HashCash (a kind of precursor to Bitcoin), and in doing so created Proof of Work, the fundamental cornerstone of BTC mining. Additionally, his writing style is very similar to that of Satoshi's from the whitepaper and forum posts. Lastly, Adam Back is the CEO of Blockstream, a company focused on building infrastructure for the Bitcoin network, such as satellites that can transmit transactions without access to the internet.

I like to think that if Satoshi is still alive, he would still be contributing to Bitcoin from the shadows. If I thought my guess would actually out Satoshi, then I wouldn't venture it. But since we're just having some fun with this one, I'm happy to share my opinion.

#12 Isn't Bitcoin mostly used for illegal activities?

Answer: If you read the headlines by the mainstream media, you may be convinced that BTC is the main source of financing for criminal groups, the dark web, buying drugs, financing terrorism, or even to hire assassins.

No. Bitcoin is not primarily used for illegal activities. In fact, according to US Department of the Treasury Deputy Assistant Secretary,

"Although virtual currencies are used for illicit transactions, the volume is small compared to the volume of illicit activity through traditional financial services."

Checkmate. If someone lobs this accusation against Bitcoin and yet partakes in traditional financial services, they are speaking from a place of either ignorance or hypocrisy.

#13 What would happen to Bitcoin if the power grid went down?

Answer: Another common question about Bitcoin is what would happen in the event of total catastrophe. While I think the question is valid, I think most people have never asked this same question about the existing financial system. It would be catastrophic. At least with USD we still have physical currency. This is largely going away, but for now, it's an advantage to have physical currency.

Having said that, Bitcoin is actually quite resistant to an event such as this. Even with a power grid down, individuals are able to use generators and solar power to charge their devices. Phones can transfer Bitcoin offline through near field communications (NFC) technology. The same thing that lets you Airdrop pictures from one iPhone to other nearby iPhones can allow individuals to transmit value.

As mentioned earlier, companies like Blockstream have created satellite infrastructure so that Bitcoin payments can be made without internet connectivity. In a really tight pinch, individuals can even load specific amounts of BTC onto what are called “paper wallets”. I could create a bunch of \$10 paper wallets and hand them out as a form of physical currency. This wouldn't be a particularly good long-term solution, but it could suffice in a survival situation to get to a point where infrastructure is rebuilt.

Bitcoin is quite resistant to catastrophic events. Human history has never seen a truly worldwide catastrophe. Bitcoin's decentralized nature makes it more resistant to such events than traditional systems because its nodes are all over the world and therefore there will always be nodes that are out of harm's way that are maintaining the network.

#14 What do I say to people who say blockchain, not Bitcoin, is the future?

Answer: One of the most popular lines among uninformed talking heads on TV and corporate executives is that “Blockchain, not crypto, is

the future.” This is another one of those topics where the very utterance of the sentence illustrates that, sadly, they are not yet fully informed on the subject.

A blockchain in its simplest form is just a ledger. Companies already have ledgers. In fact, centralized ledgers are more efficient than decentralized ones. It’s a much more cumbersome process to get all nodes to agree to new entries on a decentralized ledger. Centralized ledgers can be updated with a few keystrokes. The purpose of having a digital asset component to the blockchain is that it provides an incentive structure that enables decentralization. Would miners spend thousands of dollars to maintain the Bitcoin blockchain if they didn’t get rewarded in BTC or some other form of compensation? No, of course not.

Key point: cryptocurrencies/digital assets are required in order for a blockchain to be decentralized. Without them, there is no incentive for miners all over the world to process transactions and secure the network.

Many of the individuals that say things like “Blockchain, not Bitcoin” are often the same individuals that confuse a *distributed* ledger with a *decentralized* one. The difference may sound small, but the implications are massive. These individuals often also say things like “DLT (distributed ledger technology) is the future!” A distributed ledger just means that everyone can see the ledger. This is neat because it’s better than the opaque systems we have today, but a *decentralized* ledger is what we really want. A decentralized ledger means that not only does everyone have a copy of the ledger, but the nodes on the network have a vote in the governance of the ledger. A distributed ledger can be seen by everyone but may still be controlled by a central party. A decentralized ledger is seen by everyone and controlled by everyone (kind of like a republic).

Blockchain *and* digital assets are the future. Not one or the other.

#15 Can Bitcoin go to \$0?

Answer: Early in its life, Bitcoin had a strong possibility of going to \$0. It was relatively centralized. It was inexpensive to 51 percent attack (getting enough hashpower to overpower the other miners). But the compounding network effect and growth into the world's most secure network has since made that narrative become less and less relevant.

As pointed out earlier in the chapter, no entity has ever lost market lead after accruing a \$100B market cap. Bitcoin has accrued a MC that is over 10x that. There is no precedent for Bitcoin to lose the market lead, let alone to go entirely to zero.

At this point there are too many powerful interested parties involved. Publicly traded companies, university endowments, regulated investment vehicles like ETF's, adoption by countries, and 100M+ users are all in the game and building toward the Bitcoin Standard. At this point, it would be like saying, in 1997, that the internet is a fad and going to zero. Yes, there were people who said that but the internet had already reached escape velocity at that point. Blockchain is growing with even more inertia at an even faster pace than the internet. Bitcoin has already reached escape velocity. The prospect of going to \$0 has a chance of about 0%.

#16 What is the difference between Bitcoin and Ethereum?

Answer: One of the perplexing things to people new to crypto is that there are so many different blockchains and digital assets. It can be confusing and overwhelming. Not all blockchain projects are attempting to do what Bitcoin is doing and vice versa. Different blockchains serve different functions (and some are outright scams). For a more exhaustive breakdown please revisit chapter 6.

The #1 and #2 coins in the industry by market capitalization are BTC and ETH. Each of these is many multiples bigger than even the third biggest coin. Currently, they stand in a league of their own. BTC

aims to function as money while ETH aims to function as oil for dApps and other decentralized infrastructure. If Bitcoin is Apple Pay, then Ethereum would be the App Store.

#17 Isn't crypto just a bubble?

Answer: When people talk about bubbles, they can be referring to two different kinds. One version is what is called a “cycle bubble” and one is an “industry bubble”. The former is part of the boom and bust cycle. The 2008 housing crash is an example of this. Yes, prices inflated and the bubble popped but the industry continued on after the pop and eventually grew even bigger than before. The latter, is a type of bubble where an industry pops and never comes back; at least never returns to the heights of its mania. An example of this would be the Dutch Tulip Bubble that we covered earlier.

What most Bitcoin antagonists are accusing Bitcoin of is being an industry bubble. No. Bitcoin is not a bubble in this sense. True industry bubbles are something that pop and never come back. Like any other financial market, Bitcoin and crypto can have micro economic cycle bubbles (meaning the price can go up and come down quickly or vice versa). But Bitcoin is certainly not a macro economic industry bubble.

Bitcoin has been declared dead 434 times⁽⁵¹⁾. When you have a minute, go to 99bitcoins.com/bitcoin-obituaries/. They have listed the plethora of headlines and articles where the media has emphatically stated that Bitcoin is done forever. If Bitcoin were a true fad bubble, it would have burst once and gone away. It has died 444 times and has more users today than it had yesterday. The evidence all points to a conclusion that is quite the opposite of these headlines - Bitcoin is not a bubble, it is the foundation to tomorrow's financial infrastructure.

#18 Can Bitcoin be hacked?

Answer: One of the beautiful and powerful things about open-source technology is that everything is out in the open. On the other end, hacks do work well on closed software systems. A hack is essentially a corruption of the programming code. A hack in an open-source environment like Bitcoin would likely fail for two reasons: one, because everyone could easily notice the change to the code (since everyone can see any changes made in real time) and two, if a bug was put into the software, it would need to be updated simultaneously onto at least 51 percent of all nodes - for all intents and purposes, an impossible task.

You may see a news story about a Bitcoin user whose wallet was hacked and their funds stolen. To be clear, this does not mean that the Bitcoin blockchain was hacked. It means that an individual user made some sort of error that led to a vulnerability, leading to their password being compromised. Just like someone can hack your bank account if you are not careful with your online banking passwords, so too can someone break into your personal Bitcoin wallet if you do not use common sense. It's important not to conflate the hacking of a user with the hacking of the Bitcoin network. Those are drastically different things.

When it comes to hacking the Bitcoin protocol, one needs to consider incentives. Have you ever seen a bank heist movie where the thieves make away with a big bag of cash but when they go to open it a paint bomb goes off, marking all the bills and making them useless? This is the same thing that would happen in the event of a hack of Bitcoin. To get enough hashpower to hack Bitcoin would take tens of billions of dollars of equipment. Vast resources of people, electricity, and space would be needed. The cost would be substantial. The organization and systems put in place to orchestrate such an attack would be considerable. Mining hardware is already in such high demand that it's arguable that no amount of money could actually buy enough hardware before inventory ran out.

Even if someone could do the impossible and hack the Bitcoin network, they would be doing so to their own detriment. A hack would make the asset they spent billions to steal totally worthless overnight.

What would happen to the price of BTC if the network was genuinely hacked? The network would lose users immediately and the thieves would be left holding a sack of worthless digital coins.

In the event of such a hack, honest miners would simply fork the blockchain from the moment just before the hack and make Bitcoin 2.0. Everyone's private keys from Bitcoin 1.0 would still work. So now the hackers would need enough computational power to overpower two blockchains. Even if they could, the blockchain could be re-forked and further increase the cost to the hackers. At that point, the hackers still would not have received any financial benefit and would be waging a losing war.

So, while hacking Bitcoin in a technical sense isn't impossible, from a pragmatic point of view it is.

#19 Will CBDC's (Central Bank Digital Currencies) make BTC obsolete?

Answer: No. CBDC's will provide the greatest marketing campaign ever for Bitcoin. If government currencies are a monarchy, Bitcoin is a democracy. CBDC's will provide better financial services than our current structure, but they will come with the steep price of programmability. They will be incredibly efficient for distributing a stimulus payment as well as other entitlements, and they will be very efficient for commerce, but they will also have the ability to withdraw, freeze, or entirely seize the funds of citizens far more easily.

CBDC's may have some other cool functionality like digital receipts. Think about how when you go to the grocery store you get a paper receipt with each item you purchased itemized for your records. But when you look at your bank account statement there is just one line that says the name of the store and your total payment. CBDC's will be able to keep a digital receipt of everything you purchased. This will be convenient if you ever need to look back at a receipt - you will be able to just click a link in your wallet that opens up your itemized digital receipt. But with that convenience comes the reality that your government also knows exactly what you purchased. Most people will say, "I have

nothing to hide so I don't care." Fair enough. It's just important for individuals to understand that this functionality will exist, and to think through its potential implications.

Early skeptics of the internet said similar remarks to what Bitcoin skeptics say, "There's no way the government will allow the internet to be the wild west where just anyone can have a website. Think of how dangerous that could be!" These same people thought .coms would go away and the only permissible URLs would end in .gov.

In the same way we see .govs and .coms coexisting on the internet, we will see CBDC's and Bitcoin coexisting in our financial system going forward.

#20 Isn't bitcoin too volatile?

Answer: If you compare BTC to USD then yes, there is significant volatility. New technologies and new enterprises always have volatility. Bitcoin purists are fond of comparing BTC to BTC rather than USD. On the Bitcoin Standard, one coin will always equal one coin. It all really depends on how things are priced. Under our current but antiquated paradigm, USD reigns, but eventually, as things move to the Bitcoin Standard and are priced in Sats, the volatility will become much less.

Aleks Svetski, Founder of Amber App, had this to say about BTC's volatility:

"In the madness of crowds, bitcoin is volatile in their perception of what it's worth... but bitcoin itself is actually anti-volatile. Volatility is inherent to things like central banks: first inflation is transitory, and then it's not. Now inflation is because of people not being vaccinated... now inflation is because of global climate change... now inflation is because of toxic masculinity. That's volatility. Volatility in opinion. Volatility in policy. Volatility in everything. Whereas bitcoin is just not. It's fundamentally not volatile. It's

the only heartbeat in the world that hasn't changed. It's still what it is. It's still backward compatible for thirteen years. That's perfection. It's the relationship between a volatile world and a perfectly pristine manifestation of a heartbeat - that connection is volatile. The alpha we get out of it is that we understand that bitcoin isn't volatile. By the time the rest of the world understands it, then you won't notice the volatility anymore.”

Allow me to further illustrate Alek's point with an example. The point of this next analogy is certainly not meant to make fun of those with mental disorders, as I have a close family member with such a condition whom I love very much. But one way to think about this is as if you are a psychiatrist in a psych ward.

The status quo within that psych ward is a bunch of “crazy” people. They are unstable, erratic, and potentially dangerous. When you attempt to give them constructive advice as the doctor, it is taken as irrelevant. In a psych ward filled with volatile personalities, the one objectively stable personality is viewed by the patients as the only fish out of water - the truly stable are seen as volatile and the volatile are viewed as stable by their peers.

This is true for BTC as well. It is perfect money. Fiat currency is the crazy one. Unfortunately, right now we are living in the psych ward where USD seems stable and sane, but I think history will look back on it objectively as the crazy one.

Although BTC has achieved a market capitalization in excess of \$1T, in terms of the value of fiat currencies in the world, that is a small drop in the bucket. Being so small compared to a behemoth like the USD means that until BTC reaches a greater maturity, there will naturally be fluctuations in its value. This is also true for companies. If you want a greater potential return on your investment, you wouldn't invest in an established company like Coca-Cola, you would invest in a lesser known

startup. It's perfectly natural for newcomers to be more volatile. There could also be opportunity there as well.

A YouTuber that goes by the name of Catoshi Nakamoto aptly said,

“When you drop a pebble in a pond it makes a big ripple. When you drop it in the ocean it’s barely noticeable.”

BTC is the pond and USD is the ocean. Even when we look at BTC through the lens of a world that revolves around USD, as BTC grows to a material enough market capitalization, the swings will become less significant.

BTC as a daily currency is not ready yet. The Lightning Network may make this a reality much sooner than many people realize though. Being a daily currency isn't the only value proposition of BTC though. BTC can be a store of value and an opportunity to build transformational wealth. Remember, volatility is not always bad. Historically, BTC has been volatile to the upside - appreciating at an average rate of 178 percent per year. USD has been volatile to the downside and has lost over 98 percent of its value since the founding of the Federal Reserve in 1913⁽⁴⁴⁾.

#21 Don't we already have digital money?

Answer: People think money is already digital because they see their online bank account represented digitally. Or perhaps others believe their money is digital because they can send money to a friend via Apple Pay. But this entire system is all just a bunch of digital IOUs that represent their physical currency.

Let's revisit our earlier example from Dumb and Dumber where Jim Carey's character Lloyd Christmas has spent all the ransom money the bad guy was supposed to get. With a gun pointed at him, Lloyd attempts to pacify the kidnapper by saying, "That sir, is as good as

money, those are IOUs! You might want to hold onto this one.” He hands the bad guy a napkin with the words “IOU: \$275,000” written on it for the Lamborghini that he bought. You can see how distraught the kidnapper is at the thought of an IOU as opposed to actual stacks of \$100 bills. This scene is hilarious because the thought of IOUs rather than actually money is absurd.

Our financial and money remittance systems function in largely the same way as Lloyd Christmas’s IOU system. The physical currency is only ever periodically settled. Imagine how difficult it would be for banks and money transfer companies to constantly take truckloads of bills back and forth to their peers. Would they do this hourly? Nightly? To the user, PayPal looks like it’s a payment that is being sent instantly, but what’s really happening? Is PayPal taking an armored truck from your Wells Fargo bank branch with the \$8.95 that is going to your friend’s Bank of America branch for the latte they spotted you for? It doesn’t take a rocket scientist to see that this would be totally inefficient.

The payment processors and financial service companies simply transmit IOUs among one another. Their books update individuals’ account balances in near real time, but the actual funds are only physically settled periodically (monthly or quarterly) because of the excessive amount of effort it would take to move that amount of paper bills.

Simply put, currently, fiat currencies are physical currency that also has a digital representation. Digital assets like Bitcoin are natively digital. They are only digital. They do not bear the physical limitations of fiat currencies and therefore possess all the efficient qualities of being digital in nature.

Chapter Fourteen:

Short Answers to

Not-So-Common Questions

#1 Is the 21M supply of BTC really unchangeable?

Answer: We are supposed to say no, that it's not, because the 21M max supply is a core principle of Bitcoin. And for all intents and purposes, the 21M supply *is* unchangeable. But in a theoretical sense, there is a way it could be changed.

If 51 percent of miners got together and decided to change the source code, then theoretically, it could be changed. Although, as I've said many times thus far, it's of the utmost importance to consider incentives. A fundamental change to the source code would violate some of the deepest held principles and fundamentals of Bitcoin and would thus turn it into something that is not Bitcoin.

This is where it is important to go back and look at the incentive structure for miners. Miners make their vast profits by mining Bitcoin because of the thriving ecosystem. Theoretically, miners could increase the coin supply in an attempt to enrich themselves, but this would achieve the opposite effect and the miners know this. They may succeed in getting more coins, but the value of those coins would drop precipitously - by a far larger margin than the value of their newly increased coin supply.

Within the ecosystem, miners are the most highly incentivized people to maintain the Bitcoin ethos and values - this is how they enrich themselves. It's a beautiful self-reinforcing system.

#2 Can Bitcoin be altered so there are smaller amounts than a Satoshi?

Answer: This is a great question. If the market cap of BTC were to reach \$20T, then a Sat would be worth about 1¢. At that point, Sats would still be a reasonable value for commerce. If the BTC market cap were to exceed \$20T, it would mean that even a Sat would become too valuable for small and micro transactions. Those who have thought of this point might be concerned that BTC would no longer be able to function as a reasonable medium of exchange.

Do not worry, the Bitcoin source code can be adjusted through a consensus amongst the miners and node operators. Rather than a Sat being the smallest unit (0.00000001 BTC), something like a mSAT (Micro Sat) could be created by simply allowing BTC to become more divisible. So instead of BTC being divisible down to 8 decimals, it could be divided down to any other amount needed such as 12 decimals (0.000000000001 BTC).

#3 How will miners make money after 2140?

Answer: While this likely won't be an issue in any of our lifetimes, at some point, the minting of new BTC every ten minutes will stop. It is projected that the last BTC will be mined in the year 2140. We have discussed earlier in the book how the block reward every ten minutes is what incentivizes the miners to process transactions and secure the network.

This begs the question, "If there is no block reward, what is the incentive for miners at that point?" The answer is simple: in addition to block rewards, miners also get transaction fees. Those wishing to transact in BTC need to pay a fee to do so. When the network isn't very congested, someone might only pay a penny for the transaction. When the network is more congested and therefore there is greater competition

to get your transaction processed more quickly, you could elect to pay a higher fee. These fees go to whichever miner processes the next block.

Fees will ensure that the Bitcoin blockchain will continue to operate long after there are block rewards.

#4 Is Bitcoin the “one world currency” from Revelation?

Answer: I run in Christian circles and one of the most common questions is: “What if Bitcoin is the one-world currency referenced in the Book of Revelation?” I usually start with a dumb joke to the effect of, “If that’s true, then we are lucky to be in early because that means it’s guaranteed to be huge!” It gets a laugh about a quarter of the time.

I then follow that up with how the US dollar has been the world currency for 70 years. If you’re going to make a case for the Revelation currency, then the US dollar becoming the world currency during a convergence of the greatest war in the history of the planet, Israel regaining its nationhood, and the literal establishment of a new world order (called the Bretton Woods Agreement) is a much more compelling argument.

I then follow it up with the fact that not only could the US dollar be that currency, but isn’t it interesting that the first nation to adopt BTC - perhaps the only way to opt out of that “evil USD currency” - is El Salvador; literally translated as “The Savior”?

For the record, I don’t think that USD or BTC is the currency people refer to from Revelation. In fact, Revelation doesn’t even specifically mention a currency. A reading of some passages could be interpreted as there someday being a one world government and therefore a one world currency (doesn’t sound too crazy by today’s globalist standards) but talk of a one world currency has largely been perpetuated by tradition rather than scripture.

#5 What is the difference between Bitcoin, Bitcoin Cash, and other cryptos with the word Bitcoin in them?

Answer: Open-source technology has many wonderful attributes, many of which have been described throughout this book. Open-source also has its share of pains. One such pain being the ability to copy the source code and create a knock off version of Bitcoin. This is not detrimental to the Bitcoin blockchain, but it can be confusing for users.

Anyone can start their own version of Bitcoin in a day. They could copy the source code and start mining their coins from their own computer, this is also known as a fork of Bitcoin. They could call their new blockchain whatever they want. If they wanted to attempt to con unknowing individuals, they could call it something like Bitcoin Gold. Someone that's new to crypto might go to an exchange and see that coin listed and think, "Wow! This bitcoin only costs three cents!" They might then pay their very real funds to buy up thousands of coins, thinking they are getting a crazy good deal, but ultimately they paid for something that truly serves no purpose and will eventually go to zero.

This happened with the most prominent fork of Bitcoin called Bitcoin Cash. Roger Ver was a well-known proponent of Bitcoin in the early days. When a disagreement came up about how to proceed with certain technological upgrades to Bitcoin, Ver and other miners and developers forked Bitcoin to make Bitcoin Cash. Ver also happened to own Bitcoin.com. When the split happened, Ver's site allegedly defaulted to selling Bitcoin Cash. Presumably, many unsuspecting visitors to the site bought Bitcoin Cash assuming that it was bitcoin.

Simply put, there are many clone projects of Bitcoin out in the world but none of them have the network effects, decentralization, or the security that Bitcoin has. They are knock offs. Some are well-meaning projects that hope to improve peer to peer payments while others are outright scams.

#6 How many developers are working in the blockchain/Web 3.0 space?

Answer: Blockchain and Web3 developers are at an all-time high and growing faster than ever. Each of the past several years blockchain jobs are among the most popular on job sites like Indeed.com. Here are some of the metrics regarding developers:

- 18,000+ monthly active developers commit code in open-source crypto and Web3 projects
- 34,000+ new developers committed code in 2021 — the highest in history
- 4,000+ monthly active open-source developers work on Ethereum, 680+ open-source developers work on Bitcoin
- 20 percent + of new Web3 developers joined the Ethereum ecosystem
- 65 percent of active developers in Web3 joined in 2021; 45 percent of full-time developers in Web3 joined in 2021

Source: *The Pomp Letter*

#7 Is it possible that a BTC could become non-fungible?

Answer: This is an important question. Throughout the young history of Bitcoin, people have theorized that some BTC could become non-fungible. Remember, being fungible (one BTC always equals another BTC) is one of the tenets of both Bitcoin and sound money. Some have argued that an individual BTC could be made unique for one of two reasons: at some point it had been used for an unscrupulous purpose or that, in the era of Environmental, Social, Governance (ESG), it had been mined with power derived from dirty fossil fuels.

Think about it, if you knew that your dollar bill had been used in the sale of a human trafficking victim, you may try to get rid of that dollar bill. With USD it's impossible to know the history of each individual note, but with a perfect immutable ledger, theoretically, one could track the history of their coin to some degree. This is also true for tracking down the source of where a coin was mined. What if it was mined using coal, but you are environmentally conscious?

The reality is that BTC transactions are often not in whole coin amounts, so no coin really stays in one piece. Most coins are aggregations of smaller units of BTC reassembled. So, while tracking down the history of a coin is somewhat theoretically possible, it's certainly not practical.

With regard to BTC that are mined by "dirty sources" making the coins non-fungible; this idea just hasn't played out. Several companies have attempted renewably mining BTC and paying for special "green certifications" to sell them for a premium, but the markets have not responded well. Companies that have tried this, tend to reverse course on it quickly. They continue to mine their BTC with green sources, but they renege on paying for a green certification because the added expense does not translate into selling at a higher price. It's as if you sold coffee beans and they were actually organic, but you chose to not pay for USDA certified organic approval because your buyers wouldn't be willing to pay any more whether you had the USDA certification or not.

What we have seen so far is that BTC coins have remained fungible and theories to the contrary have remained just that: theories.

#8 Business Idea: BTC mining as a lottery.

Answer: This isn't a question, but it's a free idea for anyone that wants it. We discussed earlier in the book how BTC mining and the nonce work. If you skipped over that part or don't remember it, head back to Question #7 in the previous chapter. We discussed how BTC mining is kind of like a reverse lottery.

In BTC mining there are collectives known as mining pools. This is where smaller mining operations combine their resources together to compete with other pools or large industrial mining operations. I believe there's a substantial market of people who are intrigued by BTC mining but only have limited computational power. Maybe they only have their PC and a few smart devices laying around the house - there's no way they could ever mine BTC profitably on their own.

Professional BTC miners expect consistent returns. But individuals who are not devoting significant resources to mining might be willing to treat their foray into mining as more of a gamble. The downside risk is quite low, but the upside benefit could be life-changing. In a traditional lottery, players pay anywhere from \$1 for a ticket to hundreds of dollars for many tickets to have "better chances of winning". Sadly, statistically speaking, most people who play traditional lotteries are in the economic lower class and below the poverty line. So, a \$1-\$10 purchase of lottery tickets is a relatively significant gamble with very long odds of winning.

With creative marketing and a fun twist, a company could develop a website and mining pool where individuals could play the BTC Lottery by using their PC or devices when not otherwise used to be perpetually making guesses of the next nonce (winning lottery number). Imagine, with a traditional lottery you would have to pay \$10 to get 10 chances to get the winning number. With a BTC Lottery, even a smartphone can make 1,500 guesses *per second*, therefore giving you 90,000 chances per minute to get the winning number! What happens if you were to get the winning number? You win the next block reward currently valued over \$312,000!

How much did you pay to make this gamble? Probably less than a few dollars' worth of electricity per year, hardly something you would even notice.

Why am I willing to give away a business idea like this? I love Bitcoin because I think it will bring more freedom to humanity than any

other tool in history. And one of the fundamental tenets of Bitcoin is decentralization. If you can get hundreds of thousands or even millions of people playing a perpetual BTC Lottery that costs them almost nothing, you can usher in tremendous decentralization, ensuring that the network is even more secure and free from corruption.

Chapter Fifteen:

Reliable Sources in Bitcoin

“A genius is the man who can do the average thing when everyone else around him is losing his mind.”

- Napoleon Bonaparte

You will be hard pressed to find the individuals discussed below only talking about the BTC price in a speculative fashion. They will overwhelmingly discuss the technology, economics, and other fundamentals within the industry. When they do discuss the price of BTC, it is never in a short-sighted manner. Good information is priceless. If you’re looking for individuals to listen to, read, and follow, these people are good resources and give sensible and well thought out commentary on Bitcoin and the crypto space as a whole.

I. Andreas Antonopoulos

Andreas M. Antonopoulos is a British-Greek Bitcoin advocate, tech entrepreneur, and author. He is a host on the Speaking of Bitcoin Podcast. He wrote the acclaimed books Mastering Bitcoin and Mastering Ethereum.

II. Michael Saylor

Michael Saylor is the founder of the publicly traded company MicroStrategy. In 2020, MicroStrategy became the first publicly traded US company to hold BTC on its balance sheet. Since then, Michael has become one of the most-well known Bitcoin

Evangelists in the world. He has also become somewhat of a Bitcoin philosopher.

III. Robert Breedlove

Robert Breedlove is a freedom maximalist, ex-hedge fund manager, and philosopher in the Bitcoin space. To him, Bitcoin is fundamentally a humanitarian movement exposing the greatest con in human history: central banking.

IV. Meltem Demirors

Meltem Demirors is Chief Strategy Officer of CoinShares, the leading digital asset manager, and a cryptocurrency investor, advisor, and advocate, with a unique blend of experience in both legacy and blockchain-based finance and cryptocurrencies.

V. Anthony Pompliano

Anthony “Pomp” Pompliano is an entrepreneur and investor who has built and sold numerous companies, run product and growth teams at Facebook and Snapchat, and invested over \$100 million in early-stage technology companies. Pomp also runs one of the largest YouTube investment channels called *The Best Business Show*. His show focuses on Bitcoin and blockchain technology.

VI. Nolan Gouveia

Nolan Gouveia is a business professor at California Baptist University. He teaches courses on business, entrepreneurship, economics and blockchain. He also runs a personal finance, investing, and entrepreneurship YouTube channel called Professor G.

VII. Isaiah Jackson

Isaiah Jackson, co-founder of KRBE Digital Assets Group and the author of “Bitcoin & Black America,” thinks that bitcoin can play a crucial role in addressing economic disparity in Black communities.

VIII. Dr. Saifedean Ammous

Dr. Saifedean Ammous is Assistant Professor of Economics at the Lebanese American University. He holds a PhD in Sustainable Development from Columbia University (2011). He authored the well-known books *The Bitcoin Standard* and *The Fiat Standard*.

Conclusion:

I used the word history 137 times in this book, and for good reason. Bitcoin has historical implications. Bitcoin has made and is continuing to make history. The beautiful thing for the readers of this book at the time of its release is that we are living at a critical juncture in history where average, everyday individuals have an opportunity to be ahead of the adoption curve of a new technology and to potentially benefit richly from it. These benefits aren't just financial though. They have implications in personal and societal justice, equality and liberty. The implications of the decentralized revolution are massive.

If Bitcoin becomes adopted on a wide scale, it will have tremendous positive effects in many different areas. It's similar to Vitamin D's role in our health, it's not the only thing we need but it is vital. Vitamin D is the one supplement that someone can take that will benefit almost every cell in the entire body. By contrast, vitamin C is only absorbed in certain cells like those that aid in immune function and the repair of tissues. That's great, but almost every cell in the body has a receptor for vitamin D. This means that vitamin D deficiency is associated with the highest rates of all-cause mortality. No other factor is more associated with all causes of death like cancers, Covid-19, heart disease, diabetes and more, than not having sufficient levels of vitamin D.

So, if a nutritionist could give you only one piece of advice that would lower your chances of dying by the greatest margin, it would be to make sure your vitamin D levels are high. Sure, vitamin D is not the only thing you need to be healthy, but it's something that affects every area of your health.

Likewise, our financial system is not the only cause of all the problems in society, but if we could only fix one thing that would have the most direct impact on living standards, equality, protection of rights, liberty, and justice, it would be transitioning from an opaque and corrupt

financial system to an open and transparent one. Bitcoin doesn't fix everything but it does fix this.

Bitcoin is like vitamin D; it is a health benefit to almost every element in society.

I believe someday everyone's portfolios will be 100 percent crypto. This doesn't mean that the only thing people will own is BTC, that would be absurd. What I am saying is that cryptographic decentralized blockchain ledgers will prove to be the best and safest way to store and represent value. So, while you might have a physical asset like real estate, the ownership of it will be represented digitally. If this is true, then individuals who read the information you just read should be very excited about the opportunity they have before them.

While it's great to be excited about Bitcoin, blockchain, and digital assets as a whole, we should always make sure to instill discipline into our processes and to fight human nature's proclivity for greed. The temptation is to worship the creation and not the Creator.

It is easy to fall into the mental trap of thinking we are noble or moral because we are adopting a morally better system. But if we are not cautious, we can fall into the same trap as those that upheld the old system; instead of the system being greedy and corrupt, we ourselves can be slaves to greed and corruption. While Bitcoin will remain immune to these corruptions, we ourselves will always be susceptible. Therefore, we must renew our resolve to use our resources for the betterment of those we have stewardship over.

The Bitcoin Whitepaper.

I have included a copy of the Bitcoin Whitepaper in this book. It would be easy enough for me to recommend that you just simply google “Bitcoin Whitepaper” and read it online. But the reason I include it here is because of what we have talked much about in this book: *decentralization*.

If Bitcoin were ever attacked at mass scale and information about Bitcoin became censored, each copy of the whitepaper around the world provides an opportunity to ensure Bitcoin’s survival. Each copy of the whitepaper means that there remains a blueprint for how to construct and maintain the network. Each copy of this book sold helps to participate in the decentralization of Bitcoin. By buying this book, you have made the Bitcoin network incrementally stronger and more resistant to attack. Thank you for participating in the world’s first truly free monetary network.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

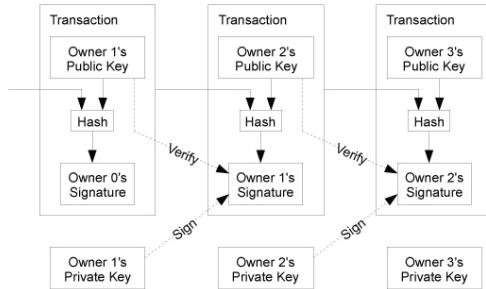
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

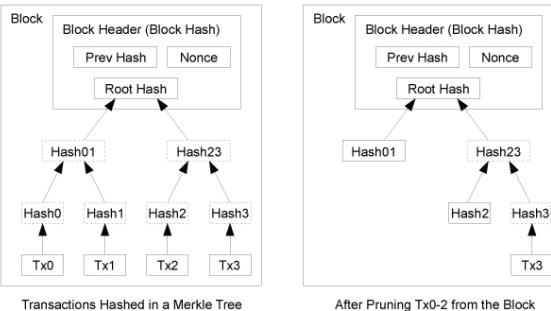
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

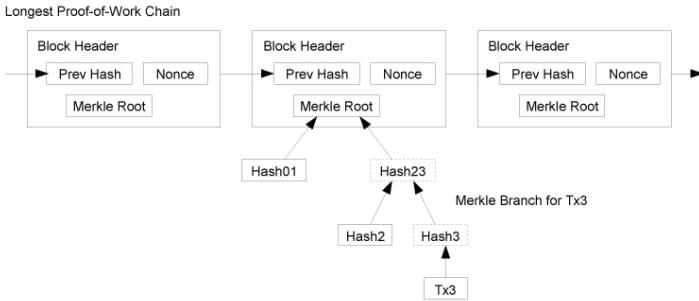
Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, $80 \text{ bytes} * 6 * 24 * 365 = 4.2\text{MB per year}$. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

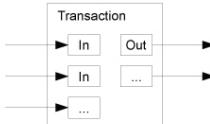
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

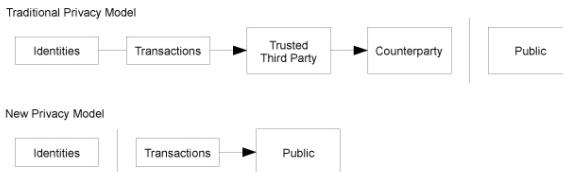
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

$$p = \text{probability an honest node finds the next block}$$

$$q = \text{probability the attacker finds the next block}$$

$$q_z = \text{probability the attacker will ever catch up from } z \text{ blocks behind}$$

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
z=0    P=1.000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10  z=5
q=0.15  z=8
q=0.20  z=11
q=0.25  z=15
q=0.30  z=24
q=0.35  z=41
q=0.40  z=89
q=0.45  z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

- [1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.
- [3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.
- [4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.
- [5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.
- [6] A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.
- [8] W. Feller, "An introduction to probability theory and its applications," 1957.

Find The BTC Wallet In This Book

Here's how it works:

BTC wallets can be secured with a 12 word “seed phrase”. These 12 words are hidden throughout the book. Once you find the 12 words (the order of the words matter), you can then download any BTC wallet you choose (Nunchuk.io, Blue Wallet, Ledger, etc), input those 12 words, and the BTC is yours!

You can find the first word pinned at the top of my Twitter account. Go to my Twitter handle [@BrianTheMint](#). You may find periodic hints and riddles through my social media channels. There you will find further instructions. Please consider following me for more content.

Happy treasure hunting!

- | | |
|----|-----|
| 1. | 7. |
| 2. | 8. |
| 3. | 9. |
| 4. | 10. |
| 5. | 11. |
| 6. | 12. |

References for Bitcoin Evangelism

⁽¹⁾ **"80% of bills have cocaine on them"**

<https://www.marketwatch.com/story/this-is-exactly-how-often-cocaine-and-feces-show-up-on-your-dollar-bills-2017-07-11#:~:text=Traces%20of%20cocaine%20can%20be,changing%20hands%20during%20drug%20deals.>

⁽²⁾ **"Americans use vastly more electric power for their Christmas lights in a single month than small countries like El Salvador or Ethiopia use in an entire year."**

<https://phys.org/news/2015-12-christmas-energy-entire-countries.html>

⁽³⁾ **"31% of adults around the world are unbanked"**

https://globalindex.worldbank.org/sites/globalindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf

⁽⁴⁾ **"6% of US households are unbanked"**

[https://time.com/nextadvisor/banking/what-to-know-if-you-are-unbanked/#:~:text=Over%206%25%20of%20U.S.%20households,Deposit%20Insurance%20Corporation%20\(FDIC\).](https://time.com/nextadvisor/banking/what-to-know-if-you-are-unbanked/#:~:text=Over%206%25%20of%20U.S.%20households,Deposit%20Insurance%20Corporation%20(FDIC).)

⁽⁵⁾ **"In the first twelve years of the internet it grew to 16M users."**

<https://www.internetworldstats.com/emarketing.htm>

⁽⁶⁾ **"In the twelve years since the creation of jewel, over 106M people have adopted it."**

<https://markets.businessinsider.com/news/currencies/crypto-users-pass-100-million-boomers-gen-x-bitcoin-btc-ethereum-2021-2>

⁽⁷⁾ **"Even the world's preeminent currency, the US Dollar, took 200 years to reach a \$1T circulating supply."**

<https://fred.stlouisfed.org/series/M2SL>

⁽⁸⁾ **Lincoln: "I have no purpose, directly or indirectly, to interfere with the institution of slavery in the states where it now exists. I believe I have no lawful right to do so, and I have no jacket to do so."**

https://avalon.law.yale.edu/19th_century/lincoln1.asp

⁽⁹⁾ **Lincoln: "My paramount objective is to save the Union, and it is not either to save or destroy slavery. If I could save the Union without freeing any slave, I would do it."**

<https://www.loc.gov/resource/mal.4233400/?st=text#:~:text=I%20would%20save%20the%20Union,shortest%20way%20under%20the%20Constitution.&text=I%20could%20save%20the,I%20would%20also%20do%20that.>

⁽¹⁰⁾ **Otto Von Bismarck:"The division of the United States into federations of equal foam was decided long before the Civil War by the high financial powers of Europe..."**

<https://www.azquotes.com/quote/615228>

⁽¹¹⁾ **12 mph and 15 mph speed limits**

<https://www.wired.com/2008/05/dayintech-0521/>

⁽¹²⁾ **Fifty years after the invention of sugar, more than 9,000,000 books were in print.**

<https://www.britannica.com/topic/publishing/The-age-of-early-printing-1450-1550>

⁽¹³⁾ **"That night, when I got into bed and closed my eyes, I had this image of all sixty thousand Blockbuster employees erupting in laughter at the ridiculousness of our proposal. Of course, Antioch wasn't interested."**

<https://www.marketplace.org/2020/09/08/ceo-reed-hastings-on-how-netflix-beat-blockbuster/>

⁽¹⁴⁾ **In 2010 Blockbuster filed for bankruptcy. That same year Netflix hit 20M subscribers.**

<https://www.cnbc.com/2020/09/22/how-netflix-almost-lost-the-movie-rental-wars-to-blockbuster.html#:~:text=By%202010%2C%20Blockbuster%20was%20forced,subscribers%20and%20started%20expanding%20over seas.>

^[15] "From 1990 to 2000, internet users grew at an average annual pace of 63%. From 2010 to 2020 blockchain users have grown at an average annual rate of 113%"

The Best Business Show, December 2021.

^[16] "Be patient. There is no need to rush, as most of the opportunity lies before us, not behind us."

https://saf.wellsfargoadvisors.com/emx/dctm/Research/wfii/wfii_reports/Investment_Strategy/cryptocurrency_020722.pdf

^[17] "Estimated to grow to \$39T by 2030."

<https://www.statista.com/statistics/216998/forecast-of-the-federal-debt-of-the-united-states/>

^[18] "In 2020, the US spent \$371B on interest payments on the national debt."

<https://www.statista.com/statistics/246439/interest-expense-on-us-public-debt/>

^[19] "This grew to \$562B in 2021."

<https://www.usnews.com/news/business/articles/2021-10-22/us-budget-deficit-hits-277-trillion-in-2021-2nd-high#:~:text=For%202021%2C%20interest%20on%20the,of%20Treasury%20securities%20higher%20returns.>

^[20] "For reference, the US spent \$725B on the entire military in 2020."

<https://www.ppgf.org/budget-basics/budget-explainer-national-defense#:~:text=The%20United%20States%20spent%20%24725,11%20percent%20of%20federal%20spending.>

^[21] "The average American keeps 33% of their wealth in cash."

<https://www.google.com/search?q=how+much+cash+does+the+average+american+have&oq=how+much+cash+does+the+average+&aqs=chrome.0.0i512j69i57j0i512l8.10072j0j7&sourceid=chrome&ie=UTF-8>

^[22] This practice goes all the way back to the Greeks in 431 B.C. when Athens debased its currency to fund their war against Sparta in the Peloponnesian War

Episode 1, The Hidden Secrets of Money

^[23] according to the St. Louis Federal Reserve's own data, it took the US 200 years to print its first \$1T. The next \$1T was printed in only 8 years. And most shockingly, from 2014 through 2021 an astonishing \$10T has been printed"

<https://fred.stlouisfed.org/series/M2SL>

^[24] According to a survey conducted by Kitco News (an investing research news site), nearly 1/3rd of Americans believe that the US dollar is backed by gold."

<https://www.economicshelp.org/blog/147600/economics/nothing-is-so-permanent/>

^[25] In the Information Age, individuals will be able to use cyber currencies and thus declare their monetary independence..."

The Sovereign Individual

Lord William Reese-Mogg and James Dale Davidson, 1997

^[26] 21.5% of businesses fail within the first year, 30% in the second year, 50% in the fifth year and 70% by the tenth year."

[https://www.investopedia.com/articles/personal-finance/040915/how-many-startups-fail-and-why.asp#:~:text=The%20Small%20Business%20Administration%20\(SBA,70%25%20in%20their%2010th%20year.](https://www.investopedia.com/articles/personal-finance/040915/how-many-startups-fail-and-why.asp#:~:text=The%20Small%20Business%20Administration%20(SBA,70%25%20in%20their%2010th%20year.)

^[27] While this meta-analysis concludes that lockdowns have had little to no public health effects..."

<https://wusfnews.wusf.usf.edu/health-news-florida/2022-02-02/a-johns-hopkins-study-says-ill-founded-lockdowns-did-little-to-limit-covid-deaths>

^[28] In a 2012 press release, the CDC stated that consistent sun exposure increases an individual's risk of skin cancer by 75%"

https://www.cdc.gov/media/releases/2012/p0510_skin_cancer.html#:~:text=Exposure%20to%20ultraviolet%20radiation%20from,getting%20melanoma%20by%2075%20percent.

^[29] Other studies have shown moderate sun exposure that contributes to healthy vitamin D levels to lower breast cancer risk by as much as 80%."

<https://www.grassrootshealth.net/blog/breast-cancer-survival-linked-vitamin-d-level/>

(30) **"The gold market capitalization (the total presumed value of all gold in existence) is \$11.489T."**
<https://companiesmarketcap.com/gold/marketcap/#:~:text=Gold's%20Market%20Cap&text=The%20Market%20Capitalization%20of%20Gold,world's%20above%20ground%20gold%20reserves.>

(31) **"At the time of writing, Bitcoin's market cap is \$785B."**
<https://coinmarketcap.com/>

(32) **"Automated Clearing House (ACH) alone payments processes north of \$5T in payments every year."**
<https://www.nacha.org/news/ach-network-moves-23-billion-payments-and-51-trillion-2018>

(33) **"According to a report by Ark Invest, in 2021 Bitcoin's worldwide payment settlement increased by 463% over 2020 (\$2.3T to \$13.1T)."**
<https://www.coindesk.com/business/2022/01/25/cathie-woods-ark-invest-predicts-bitcoin-could-exceed-1m-by-2030/>

(35) **"A 3 year study by NFX, network effects accounted for 70% of the value in tech companies over the last 20 years."**
<https://www.nfx.com/post/70-percent-value-network-effects>

(36) **"The top 100 companies on the NASDAQ (the exchange for the world's biggest tech stocks) have a cumulative value of \$15T."**
<https://www.nasdaq.com/nasdaq-100>

(37) **"Encyclopaedia Britannica, the preeminent encyclopedia company's highest annual revenue was \$72.9M."**
https://growjo.com/company/Encyclopaedia_Britannica

(38) **"Google, the preeminent search company's highest annual revenue was \$75.32B."**
<https://www.nytimes.com/2022/02/01/technology/google-alphabet-earnings.html#:~:text=But%20one%20thing%20has%20not,percent%20from%20a%20year%20earlier.>

(39) **"According to bankrate.com Nearly half of millennials (49%) are at least somewhat comfortable with investing in crypto assets such as Bitcoin, compared to 37% of Generation X and only 22% of Baby Boomers"**
<https://www.bankrate.com/investing/survey-millennials-cryptocurrency-investing-2021/>

(40) **"83% of millennials held at least some digital assets."**
<https://www.cnbc.com/2021/12/16/millennial-millionaires-plan-to-add-more-crypto-in-2022.html>

(41) **"Millennials are set to inherit \$30T over the next 20 years."**
<https://www.openinvest.com/articles-insights/30t-in-inheritance-moving-to-millennials-how-to-prepare-you-r-business-for-this-great-wealth-transfer>

(42) **"Americans use more electricity in the month of December on Christmas lights than small countries like El Salvador Ethiopia and Tanzania use in an entire year."**
<https://www.npr.org/sections/goatsandsoda/2015/12/22/460699220/what-burns-more-kilowatt-hours-americas-xmas-lights-or-tanzania#:~:text=A%20headline%20for%20a%20chart,the%20developing%20world%20are%20paltry.>

(43) **"Efficient miners can mine a BTC for about \$9,000, on average."**
<https://minerdaily.com/2021/how-much-does-it-cost-to-mine-a-bitcoin/>

(44) **"USD has been volatile to the downside and has lost over 98% of its value since the founding of the Federal Reserve in 1913."**
<https://www.buybitcoinworldwide.com/dollar-devaluation/>

(45) **\$12.4B was spent on Overdraft fees in 2021**
<https://www.forbes.com/advisor/personal-finance/how-to-prgeorgeevent-overdraft-fees/>

(46) **After WW2, the US held 75% of the world's gold**
<https://www.investopedia.com/ask/answers/09/gold-standard.asp#:~:text=At%20the%20end%20of%20WWII,own%20high%20demand%20for%20imports.>

⁽⁴⁷⁾ **Bitcoin to Sat Chart**

Cointelegraph

⁽⁴⁸⁾ **Blockchain chart**

Investopedia

<https://www.investopedia.com/terms/b/blockchain.asp>

⁽⁴⁹⁾ **Peer to Peer Money Illustration**

Crypto Explorer

<https://m.facebook.com/cryptoexplorerchannel/>

⁽⁵⁰⁾ **China has banned Bitcoin 6 times**

<https://99bitcoins.com/bitcoin-obituaries/>

⁽⁵¹⁾ **Bitcoin has died 434 times**

<https://99bitcoins.com/bitcoin-obituaries/>

⁽⁵²⁾ **Prime Minister Justin Trudeau praises China's "basic dictatorship".**

<https://www.breitbart.com/politics/2022/02/15/watch-justin-trudeau-expresses-admiration-for-china-in-resurfaced-video/>