

Gradually, Then Suddenly

A Framework for Understanding Bitcoin as Money

PARKER A. LEWIS

Copyright © 2023 by Parker A. Lewis

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopy, recording, or any other—except for brief quotations in printed reviews, without the prior written permission of the author.

Original cover art by Proof of Paint,
which was commissioned for *Gradually, Then Suddenly* by Parker Lewis.

ISBN: 979-8-218-29287-4 (hardcover)
ISBN: 979-8-218-29288-1 (ebook)

Table of Contents

FOREWORD	v
INTRODUCTION	1
PART I: THE FUNDAMENTALS	25
1. Bitcoin Obsoletes All Other Money <i>First Principles of Money</i>	27
2. Bitcoin, Not Blockchain <i>A Foundation to Eliminate the Noise</i>	53
3. Bitcoin Is Not Backed by Nothing <i>What Secures Bitcoin's Fixed Supply</i>	69
4. Bitcoin Is Antifragile <i>Gaining Strength through Adversity</i>	93
5. Bitcoin Is the Great Definancialization <i>The Implications and Consequences</i>	115
PART II: COMMON MISCONCEPTIONS	141
6. Bitcoin Cannot Be Copied <i>Finite Scarcity Only Happens Once</i>	143
7. Bitcoin Is Not Too Volatile <i>Volatility Does Not Prevent Adoption</i>	153
8. Bitcoin Does Not Waste Energy <i>Scarcity Requires Real-World Cost</i>	169
9. Bitcoin Is Not Too Slow <i>A Fixed Supply Is the Zero to One Innovation</i>	181
10. Bitcoin Is Not for Criminals <i>Censorship Resistance Is All or Nothing</i>	199

11. Bitcoin Cannot Be Banned <i>A Currency System beyond Governments</i>	211
12. Bitcoin Is Not a Pyramid Scheme <i>Supply Constraints and Fundamental Demand</i>	223
PART III: BITCOIN VS. THE DOLLAR	233
13. Bitcoin Fixes This <i>The Solution to Money Printing</i>	235
14. Bitcoin Is a Rally Cry <i>The Only Viable Path to Opt Out</i>	247
15. Bitcoin Is Common Sense <i>Simplicity vs. Complexity</i>	259
16. Bitcoin Is One for All <i>The Most Equitable System for Everyone</i>	277
PART IV: CONCLUSION & ACKNOWLEDGMENTS	311

FOREWORD

Gradually, Then Suddenly

By Marty Bent

The fall of 2008 was a formative time for a lot of people around the world. The financial system was crumbling, there were worries that banks were going to run out of money, people were losing their jobs, and public officials were scrambling to figure out a way to hold everything together. Ultimately, the solution to ensure that the world didn't completely fall apart was for central banks and governments to embark on an unprecedented campaign of bailouts and money printing—socializing losses of Wall Street investment banks that stemmed from poor risk management. Emergency measures, which started with the Toxic Asset Relief Program (TARP) and quantitative easing, snowballed into a decade of monetary expansion and artificially low interest rates that led to a massive misallocation of capital and asset price inflation.

It is all a bit poetic when you think about it. The fall of 2008 can be interpreted in two ways: as a seasonal marker of the time of year when everything blew up, or a marker of greater significance that represents the complete and permanent departure from any semblance of sane monetary policy. The response to the Great Financial Crisis marked a point of no return. The powers that be could have made the hard decision to let the markets clear and wipe out all of the bad debts in the system, but instead, they chose to double down on the madness—creating a system of ever more perverse incentives that have only exacerbated the original problems underlying the crisis. The normalization of bailouts and money printing that began in 2008 sent the United States down a path of monetary ruin that

cannot be walked back or undone. The fiat system is too far gone to be fixed. As our good friend Parker likes to say, “There is simply too much debt and not enough dollars.”

Luckily for me, as fate would have it—just as the global financial system was melting down—I was a seventeen-year-old high school senior taking an economics class taught by a professor of the Austrian School who viewed the Great Financial Crisis as an incredible opportunity to illuminate our class about just how messed up the fiat system had become. Mr. Robson had us poring through the TARP bill to highlight all of the “pork” we could find in the form of handouts, unnecessary laws, and unrelated spending that got swept into the bill by politicians who saw TARP as an opportunity to get their special interests financed. *Never let a good crisis go to waste.*

As one might expect, everything about the response to the crisis left a very bad taste in my mouth. Beyond the TARP bill, Mr. Robson pointed out the insidious nature of the bailout process and had us asking questions like: Why did they let Bear Stearns and Lehman Brothers fail, but not Goldman Sachs or JP Morgan? Who is going to pay for this at the end of the day? Why do taxpayers have to pick up the \$700 billion bill when the big banks got us into this mess? What’s to prevent this from happening again in the future? All very heavy questions for a naive seventeen-year-old to ponder as he was simultaneously watching his father silently struggle through the crisis as someone who had built his career in the asset management business and had been negatively affected by the market implosion.

Needless to say, this was a formative period of my life. How could everything be so broken and corrupt?

Funnily enough, around the same time I was having my formerly naive worldview completely shattered while sitting at my desk in Mr. Robson’s class, Satoshi Nakamoto emerged out of the ether to let the world know that he had been “working on a new electronic cash system that’s fully peer-to-peer, with no trusted third parties.” The fully peer-to-peer electronic cash system with no trusted third parties was called bitcoin, and it changed the course of human history when it officially launched in January 2009.

I didn’t come across bitcoin until I was a junior at DePaul three years later, and I don’t even recall exactly how I initially got exposed to it. However, I do remember being immediately drawn to the idea of a form of money that existed beyond the control of governments. I certainly didn’t have a full grasp of how bitcoin worked when I stumbled upon it, but I had an intuition that it was something I should take the time to understand. Back in that era of bitcoin, the resources to learn about the protocol and its implications were severely limited—from bitcointalk.org to Twitter, Reddit, a few poorly produced podcasts, some YouTube channels, and (thankfully) the Satoshi Nakamoto Institute. There was a lot of noise at the time, and it was truly hard to get a firm grasp on what was actually happening.

There were people saying that bitcoin would not work because the government would never allow it. Others would deride bitcoin for being too cumbersome and slow to fulfill the role of the world reserve currency. There was always a new, “shinier” object that had improved (supposedly) on bitcoin’s original design to bring the market what it actually needed. The “distributed ledger technology” was the real innovation. Bitcoin was just a rough prototype—so said the critics.

It took me a long time to get my bearings in the world of bitcoin, altcoins, and “blockchain technology.” After many years of deep research, contemplation, and traveling down the path set forth by many pied pipers—affinity scammers who emerged in the wake of bitcoin’s success—I finally came to the conclusion that bitcoin was (and is) the only thing that matters in the world of “crypto.” Bitcoin is a form of money that no one can print or control and that is of immense value to the entire world. While I do not regret the path I took to reach that conclusion, I also do not think it is a journey that everyone should similarly suffer. As it stands today in 2023, there has never been a better base of educational content for people to arrive at the realization that bitcoin is the best form of money humans have ever come into contact with, and in my humble opinion, there is no better “zero to one” primer that explains what bitcoin is, how it works, why it’s important, and why it likely won’t be usurped than Parker Lewis’s *Gradually, Then Suddenly*.

This book addresses all of the questions I spent years trying to answer. Is bitcoin viable as money? Why bitcoin, not blockchain? How can we be sure it isn't a Ponzi scheme? Why can't bitcoin be copied? Why does bitcoin use so much energy? Why are blocks only produced every ten minutes? Can we really run a global economy using a form of money with a hard-capped supply? Parker methodically explores all of these questions and more with concise articulation that is unrivaled.

I'm excited for you. I really am. I am extremely fortunate to be able to call Parker a close friend and mentor. My journey from Mr. Robson's class to bitcoin came full circle years later when I read a research paper Parker wrote on the financial crisis, quantitative easing, and why the Fed was always going to have to print more money. It all fit into place. The paper articulated ideas I knew (or sensed) to be true but in a way that allowed me to see the problems of the broken fiat system more clearly than ever. Soon thereafter, Parker began writing about bitcoin as the solution. Through our friendship and his writing, Parker has helped me develop a better understanding of bitcoin, monetary economics, how to block out the noise that comes with "crypto," and how we are going to rebuild the economy under a bitcoin standard. We're at the early stages of a tectonic shift for humanity, and whether you realize it or not, bitcoin is at the center of that shift. While it may not feel like it, it is *morning* in America.

Bitcoin presents us with the opportunity to build a new monetary system in parallel to the incumbent system as it nears its death throes. We are incredibly fortunate that bitcoin was conceived when it was and that it has thrived ever since its launch. No longer does anyone have to depend on central planners to properly manage the money (and money supply). Bitcoin is an empowering tool that gives each of us a voice and a path to opt in to a more stable economic system. Everyone who adopts bitcoin—whether to save wealth or conduct commerce—is at the same time expressing both a vote of confidence in its monetary principles and a vote of no confidence in the fiat monetary system.

Bitcoin is a fully transparent open-source software project that enables anyone who is so willing to contribute—whether it be via improvement

proposals, code reviews, education, building infrastructure, or simply saving. Under fiat systems, everyone is subject to the whims of unelected academics who think they are smarter and “holier than thou.” It doesn’t have to be that way anymore. The bitcoin network returns sound money to the world. It is a beautiful thing that most people either take for granted or simply do not understand.

I have a feeling that by the time you are finished with this book, you will come to the same understanding. So, go forth and enjoy the eye-opening journey you’re about to take. It will be much smoother than the one I took to get to this point.

INTRODUCTION

Gradually, Then Suddenly

(Authored March 2023)

Perfect Timing

On March 12, 2008, CNBC reporter David Faber asked Bear Stearns CEO Alan Schwartz to respond to reports that Goldman Sachs “would not accept the counterparty risk of Bear Stearns.” Within a few days, the collapse of the Wall Street investment bank was complete. The Federal Reserve and US Treasury Department stepped in to engineer a bailout, which ultimately came through an acquisition by J.P. Morgan. Bear Stearns was the first major domino to fall in the 2008 financial crisis, but the entire financial system was on the verge of collapse. Six months later, on September 15, 2008, Lehman Brothers filed for bankruptcy. This time there was no bailout. The bank runs were on in full force across Wall Street. Within a few weeks, President George W. Bush passed the Emergency Economic Stabilization Act, signed into law on October 3, 2008, approving a \$700 billion package to bail out major US banks.

No one could have predicted what would happen next. On October 31, 2008, a shadowy super coder working under the pseudonym Satoshi Nakamoto sent an email to a cypherpunk mailing list, sharing a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System.” On January 3, 2009, bitcoin was officially launched, and the world would be changed forever. Satoshi mined the first bitcoin block inscribed with the text, “the Times 03/Jan/2009 Chancellor on brink of second bailout for banks,” the

front-page headline of the *Times of London* for that day—a timestamp with a message. Within less than a week, the code was publicly released. A day later, California software developer Hal Finney became the first known person to join the network, tweeting two simple words: “Running bitcoin.” The rest is actively becoming history.

Just as the financial system was on the brink of collapse, a new system was put forward that would fundamentally fix the root cause. At the time, I was working at Deutsche Bank, just down the road from the New York Fed, at 60 Wall Street. I had a front-row seat to the chaos that was the Global Financial Crisis. Admittedly, it was impossible to know what was really happening or why. Something was fundamentally broken, but beyond that, it was unclear what exactly had gone wrong. I had no knowledge of bitcoin’s release and would not become interested in it until 2016. During that time, I began to understand what had caused the financial crisis and what the implications would be going forward. In hindsight, it has become clear that bitcoin was purpose-built to fix what was broken—the money and the financial system built on top of it. The right place at precisely the right time.

The financial crisis was triggered by extreme levels of leverage, built up over decades. This leverage was both unnatural and unsustainable. It could not and would not have existed without the function of a central bank with the ability to create money. Moral hazard was everywhere, and everything broken in the financial system could be traced back to a central bank with the unilateral power to print money. The only logical solution to an economic system plagued by a form of money that can be easily printed is one built on a form of money that cannot. This is what bitcoin ultimately represents. A form of money that cannot be printed—at all or by anyone—and an entirely new economic system is being built on top of it. While the idea of a digital cash system had been around for decades, none had ever worked. A system built on trust was broken, and Satoshi put forward the idea of a system that eliminated centralized third parties from the issuance and settlement of money. Essentially, bitcoin could only work if it removed the need for trust entirely.

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.

—Satoshi Nakamoto, February 2009¹

Ever since its release, bitcoin has been hiding in plain sight for all to see, yet it remains difficult to see. The same is true of the issues stemming from the legacy system. Every day, more people figure it out, but the overwhelming majority of individuals remain in the dark. Skepticism is logically high. Bitcoin is a better form of money that will replace all other currencies, including the US dollar? The idea sounds outrageous. Warren Buffett has referred to bitcoin as rat poison—or more specifically, rat poison squared. Charlie Munger, Buffett's longtime partner at Berkshire Hathaway, has taken to the Wall Street Journal to deride bitcoin as an evil scourge, arguing it should be banned. Munger even praised the leader of the Chinese Communist Party for pursuing measures to make its use illegal. JP Morgan CEO Jamie Dimon has called bitcoin a fraud on multiple occasions. Many political leaders in the US, from sitting senators to congressmen, presidents, and cabinet members, have warned that bitcoin is a national security threat or otherwise dismissed it as nothing more than a pet rock.

Despite its critics, bitcoin exists and continues to operate fourteen years after its launch. Today, bitcoin has a purchasing power of approximately \$480 billion, ranking it somewhere around the twenty-second largest currency system in the world. People may think of bitcoin as new, niche, or nascent, which is not inaccurate, but bitcoin is significant at the same time. It may be small relative to the legacy financial system, but it is also material in size. It has been in the wild for over a decade, processing transactions

1. Satoshi Nakamoto, "Bitcoin Open Source Implementation of P2P Currency," P2P Foundation, forum post, 11 February 2009.

without fail and without anyone in control. And adoption continues to grow. Individual after individual who intentionally and consciously evaluates bitcoin consistently arrives at the conclusion that bitcoin is a superior form of money.

The question to ask yourself is *why*? No matter how confusing bitcoin may seem, it is upon each individual to explain the reality that exists in front of them. It does not matter if most people in the world do not understand bitcoin. Even if 999 out of 1,000 people cannot fathom or explain how bitcoin could be money, what explains the emergence of a consensus among millions of people that runs counter? Truth and objectivity exist in the world, and the only way to explain how millions of people have arrived at the consistent endpoint that bitcoin is money is through reason and logic. Either everyone is collectively hallucinating, or an objective truth exists that allows each to come to the same answer. One or the other.

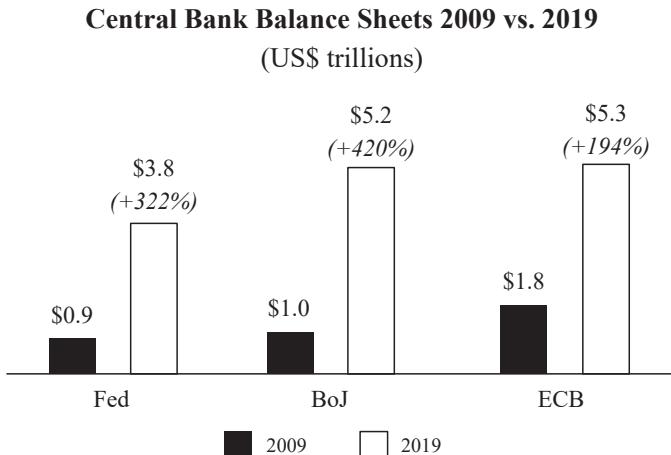
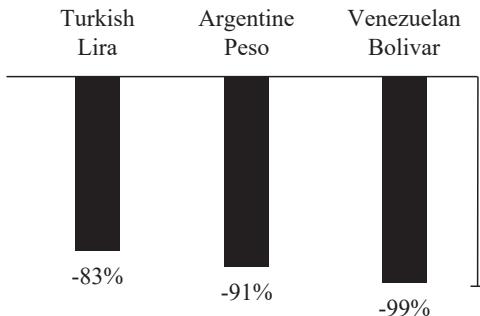
In the 1841 book *Extraordinary Popular Delusions and the Madness of Crowds*, Charles Mackay wrote about the Dutch tulip bubble, an episode in history to which bitcoin is often compared, as a hallmark example of mass delusion. Rare tulips traded at ever more extreme prices, reaching multiples of the average person's salary, followed by a crash back to reality as the speculative craze subsided. Speculative asset bubbles can and do exist. Markets can also persist in irrational states for extended periods. While the tulip bubble lasted only three years, bitcoin remains either a popular delusion or the output of rational thought. It cannot be both.

This book is intended to help readers establish a rational and logical framework from which to understand bitcoin as money—to see what is otherwise difficult to see. The only way for anyone to consistently arrive at the same conclusion about anything—let alone bitcoin—is through reason and logic. When evaluating bitcoin, this is also the best way to determine whether everyone else is crazy. If you cannot arrive at the conclusion that bitcoin is money through reason and logic, then it is more likely just a popular delusion. However, the reverse is also true.

Bitcoin Is Money—My Journey, Reason, and Logic

Bitcoin is money. Or rather, bitcoin has become money to me. It was a slow process and one that required me to break through a number of mental blocks along the way. But it all began with asking the question: *what is money?* That is the beginning of the real rabbit hole. At the root level, it is an attempt to answer the question, *why is the dollar in my pocket money?* Why do hundreds of millions of people exchange their hard-earned, real-world value every day for a piece of paper (or digital deposit)? These are difficult questions to ask and even harder ones to answer. I realized that everyone has to approach it in their own way, on their own timeline, and guided by their own life experiences. But people must first be interested in that question—what is money—to begin to understand bitcoin.

For me, the path involved first understanding why gold had emerged as money over thousands of years. What properties made one form of money better or worse than another, and what differentiated money as a unique economic good when compared to all other economic goods? *The Bitcoin Standard* (2018) by Saifedean Ammous was a formative resource for me in exploring these questions. When I applied the core principles to my own life experiences and separately to my understanding of the legacy financial system, bitcoin started to become intuitive. As part of my process, I found it helpful to consider bitcoin relative to two tangible guideposts: gold and the dollar. Does Bitcoin share the properties of either gold or the dollar? Is bitcoin *better* than either or both? Because what makes something money is not absolute. Money is an A/B test. It is a choice between storing value in one medium rather than another, which always involves trade-offs. Without first understanding the flaws of the legacy financial system and the currencies native to it (be it the dollar, euro, yen, pound, bolivar, peso, lira, etc.), I could never have arrived at the idea of bitcoin being money in a vacuum.

**FIGURE 0.1****Emerging Market Currencies vs. US\$ 2009–2019**
FIGURE 0.2
Source: Yahoo Finance

In 2016, the Federal Reserve had signaled plans to remove liquidity it had injected into the financial system in the years following the Great Financial Crisis—approximately \$3.6 trillion from 2009 to 2014, increasing the money supply fivefold. At the time, I was trying to understand the impact this would have on financial markets, and to do so, I needed a better understanding of why the Fed had taken these emergency measures in the first

place. My research led to the realization that, prior to the crisis, the financial system had been leveraged 150 to 1, the ratio of total debt in the US credit system to dollars available to banks. There was too much debt and too few dollars. The liquidity provided by the Fed, often referred to as quantitative easing (QE), was designed to prevent the collapse of the credit system. However, it became apparent that QE not only prevented deleveraging but also caused an unsustainable credit system to metastasize. I came to the conclusion that the Fed was always going to have to print more money, in massive quantities, functionally without end. QE led to more QE. I recognized that this was a problem because it would eventually lead to a complete failure of the currency.

On one hand, the Fed was going to have to print a lot more dollars, and on the other, I began to form a perspective as to why bitcoin had fundamental value, which was directly related to the problem of printing money. In the simplest terms, bitcoin derives value from the fact that it has a fixed supply. It represents a form of money that cannot be printed. There will only ever be 21 million bitcoin. As I developed a deeper knowledge of how bitcoin credibly enforced its fixed supply, I came to the principal conclusion that bitcoin was the solution to the dollar—and more generally, to the problem of printing money. My thought process followed simple logic: if bitcoin credibly enforces its fixed supply of 21 million, then it will emerge as the global reserve currency and will replace the dollar entirely. I also connected that the logic was binary. If bitcoin could not enforce its fixed supply, then it would not emerge as money. It would not be a global reserve currency, and it would not replace the dollar. Everything hinged on whether or not bitcoin could *credibly* enforce its fixed supply. Understanding how and why this is possible is the basis of understanding bitcoin as money.

There are two economic principles (or assumptions) that connect the dots between the importance of a fixed supply and global adoption of bitcoin as money, both of which will be explored in detail in the chapters to come. First, scarcity in supply is key to a currency's ability to store value over time, and second, economic systems converge on one form of money. If both

are true, the world will converge on the scarcest form of money for the reason that it will store value better than any other form of money. Economic systems converge on a single form of money due to the nature of trade—the intersubjective problem money helps to solve. At the most basic level, I must have the form of money you are willing to accept in order for us to trade or exchange value. It is not a coincidence that local economies overwhelmingly facilitate trade in one common currency because the identical problem extends out to every person in the economy. It is also not by random chance that one form of money emerges over another. There is rhyme and reason. The form of money that is hardest to produce wins, provided it is widely accessible and capable of facilitating exchange. Bitcoin is global, permissionless, and finitely scarce, and it can be transacted over a communication channel. It is outcompeting all other currencies, including the US dollar, based on the credibility of these properties in aggregate.

In the essays that follow, I lay out the logical case for readers to further connect these dots. Or rather, I will provide my logic and the framework that allowed me to consistently arrive at the most fundamental conclusions about bitcoin. Understanding why bitcoin's fixed supply is relevant is just as important as understanding how it is credibly enforced. By the end, you will have a framework with which to form your own conclusions about a number of key questions surrounding bitcoin. Is bitcoin money? If bitcoin can credibly enforce its fixed supply, will it emerge as the global reserve currency? Can bitcoin credibly enforce its fixed supply?

Historical Context

This book is a collection of essays originally published from July 2019 to December 2020. I titled the series *Gradually, Then Suddenly*, which is a common adaptation of how Hemingway described the process of going bankrupt. It's also the way that government-backed currencies hyperinflate, and often how people come to understand bitcoin (gradually, then suddenly). I wrote the essays as standalone pieces, on a specific subject or concept, with the idea that

anyone could read a single essay without needing any prior knowledge of the others or bitcoin. I have packaged the essays in this book in a more linear order to create a roadmap for the reader, but I have also preserved the original idea of the series. Each essay is designed to be read as a standalone, and collectively, the essays provide a comprehensive framework for understanding bitcoin. In order to explain certain concepts, there is some built-in redundancy but only to the extent necessary to help the reader establish a grounding to think about a particular principle or question.

I have preserved the essays in as close a form and substance to the originals as possible for intentional reasons. While I have edited the essays for copy, readability and to better knit them together (or eliminate unnecessary redundancy), the historical context of when the pieces were written was and remains relevant. Historical narratives often shift to adapt to inconvenient facts, which turn out to be inconsistent with original arguments. I was sensitive to this and did not want the reader to be left wondering whether the narrative of a particular essay shifted based on a changing set of facts. For people who have read these essays and might want to pass the book along to family and friends, I also wanted to provide an assurance that the form of essays included herein are holistically consistent with, and substantively the same as, the originals.

When I was researching the issues related to the Federal Reserve and the US dollar system in 2016, I went back and read Fed meeting transcripts from the period during and following the Great Financial Crisis. Federal Reserve transcripts are released five years after the actual meetings take place and provide a verbatim record of the discussions that occurred. I found the exercise to be particularly valuable because it provided a unique historical context and objectivity for the reader. It was like reading a story where the main characters did not know the ending, but the reader did. People can debate the benefits or detriments of the Fed printing money, but the Fed meeting transcripts provide a historical account that is not editorialized or altered. When I read the transcripts, I had the benefit of knowing what actually happened with a minimum of five years having passed. The preservation

of a historical record provided a baseline to objectively evaluate how accurate the experts were and whether the experts were really experts at all. The passage of time was also critical to the evaluation.

This is the spirit with which I have packaged the *Gradually, Then Suddenly* series of essays here. To provide historical context to the reader, I have included the original publication dates. In substance, the essays have not changed, and the original form of each essay is also preserved online under the same titles as a source of truth and comparison. As such, anyone reading these essays for the first time has the benefit of time and more knowledge of world events than I had when originally writing. For example, the Fed began printing money once again in September 2019 and proceeded to print (or digitally create) nearly \$5 trillion new dollars from 2019 to 2021. In the months leading up and without the knowledge that this would occur, when it would occur, or the extent to which it would, I wrote essays in which I explained principles as to why the Fed would need to print more money. I also wrote several essays in the midst of the then-latest money-printing epoch, describing the consequences and contrast to bitcoin. In short, the historical context is relevant.

By preserving the historical record, I believe the reader will be in the best position to evaluate the arguments, through reason and logic, and to ultimately judge for themselves—in a way that would not be possible without the passage of time since original authorship. It is an exercise of using the past to inform and evaluate what is expected to occur in the future, with logical explanations as to why. Each essay is also principles-based and as such, is just as timely today as when first authored and published. Ultimately, there was nothing to lose and much to gain by preserving the historical record and substance of the original versions.

Content Roadmap

The essays have been organized in three sections: The Fundamentals, Common Misconceptions, and Bitcoin vs. the Dollar.

Focus on the fundamentals, first and foremost. Of all the sections, I would recommend reading the essays in the Fundamentals section in the order presented. While each can be read as a standalone without prior knowledge of the others, there is a logical progression of principles from essay to essay. The Fundamentals covers high-level ideas to help readers establish a bottom-up understanding of bitcoin—defining the core properties that allow money to functionally coordinate trade, explaining how these properties exist in bitcoin, and discussing how the financial system will change as a result of global bitcoin adoption. This section also demystifies what a blockchain is, why a blockchain is only viable in the application of money, and consequently, why only bitcoin’s blockchain is relevant or valuable. Certain essays describe how bitcoin works at a technical level to ground the reader in a fundamental concept. However, each is written in such a way to be accessible to non-technical readers. This section collectively answers the fundamental questions regarding what money is, why economic systems naturally converge on one form of money, how bitcoin secures its fixed supply, why bitcoin’s fixed supply is so relevant to adoption, and why the entire world is converging on bitcoin as money.

While you are reading about the fundamentals, many questions will naturally and logically arise, particularly those that stand in opposition to the ideas presented. As questions come up, I would recommend referencing the Table of Contents to address each question as it arrives, even if it means pausing and not completing a particular essay. Understanding bitcoin is as much an exercise of removing mental blocks as it is building a foundation. Everyone needs some grounding in the fundamentals to objectively and independently consider the common questions, misconceptions, or criticisms. But working through each common criticism of bitcoin is a necessary step in establishing a better grounding in fundamental concepts. The Common

Misconceptions section should address just about any question or concern that logically arises, but each is also tied back to a fundamental concept.

For example, “Bitcoin Obsoletes All Other Money” is the most bottom-up of all the essays. As you read about the basic building blocks explaining why the entire world will adopt bitcoin as money, you may find yourself thinking, *but bitcoin is too volatile to be money*. Whereas the fundamental essay is focused on the inputs that create demand, “Bitcoin Is Not Too Volatile” is structured to help the reader think through the specific concept of volatility and why volatility does not prevent bitcoin adoption. Separately, in “Bitcoin, Not Blockchain,” I explain why a blockchain is only valuable or viable in the application of money and that economic systems converge on a single form of money. I also explain that bitcoin requires a significant amount of energy resources, by design, to secure the network. This often raises questions. If the entire world adopts bitcoin, how much energy will bitcoin consume? Is that sustainable? In “Bitcoin Does Not Waste Energy,” I lay out a framework to think about the energy resources that bitcoin demands and why this is not only sustainable but also critical to society beyond bitcoin as an application.

Naturally, the same consistent questions come up for people who are seeking to understand bitcoin on a deeper level. While it’s impossible to know which will come up for each individual and in what order, the same questions arise because they are logical to ask—but every question has an answer. Or rather, a framework to ground the reader back in the fundamentals through reason and logic. While the Common Misconceptions section is ordered in the most logical progression, there really is no way to predict which will come to the reader or when. Most importantly, recognize that everyone who has begun to understand bitcoin as money has had to cross the same bridge before you. Everyone has had to struggle through the same challenging questions. That is how bitcoin becomes intuitive. Building block by building block. One step at a time and one question at a time.

One of the most significant questions relates to problems inherent in the legacy financial system, which is why an entire section is devoted to Bitcoin vs. the Dollar. While most people do not understand that a problem even exists,

some may sense that something is fundamentally broken, but not specifically what. Others may understand that creating money out of thin air does not make sense, without recognizing the critical nature of the problem or that bitcoin is a solution. While much of my writing is focused on comparisons between bitcoin and the dollar, and geared toward a US audience, it applies broadly to currencies worldwide. On my own journey, understanding that the dollar was irreparably broken, independent of bitcoin, allowed me to recognize that I personally needed a solution. That same problem applies globally, to each individual, to each community, to each company, to each country, and especially to the US. Not everyone will need the same grounding in the issues of the legacy system to understand why bitcoin is a superior form of money, but for most, this is a critical anchoring point.

While I weave in elements of the issues inherent to the dollar (and the legacy system) throughout many of the essays, the section on Bitcoin vs. the Dollar delves deepest into the fundamental problems of printing money. I wrote the first of these essays just weeks before the Fed unexpectedly began its 2019–2021 mass-scale money-creation epoch. In the essay, I explained that “future QE is not merely a possibility; it is a certainty. Future QE from the Fed, and central banks all over the world, is a ‘when’ not ‘if’ question.” The remaining essays were written over the following twelve months, a period during which the Fed created over \$3 trillion in new base money. I discuss the reasons why this occurs, why it will always persist, what the consequences are, and most importantly, why it is a problem that must be fixed. For those who already accept that printing money is a problem that needs solving, this section will only be valuable if you want to understand the issues at a deeper level, and it will be less critical to understanding the fundamentals of bitcoin as money.

In all cases, anyone who adopts bitcoin as money will still need to navigate the chaos created by the Fed and its monetary policy, which functionally affects the entire world. There is no avoiding the fallout, and Fed actions will continue to impact all aspects of the economy, including bitcoin, for the foreseeable future—which is why this section is highly relevant

beyond bitcoin. The Fundamentals and Common Misconceptions sections are most important to building a bottom-up framework for understanding bitcoin, but bitcoin also cannot be understood in a vacuum. As such, I would recommend consuming the essays from this section either as supplementary resources or to the extent that questions about the dollar rise to the forefront for you.

Goals for the Reader

Bitcoin is hard to see but impossible to unsee once the picture comes into focus. At the start, it is the furthest thing from intuitive. But then something will click for you. Some idea will land that allows bitcoin to become possible in your mind. It starts with a *maybe*. Maybe these people aren't all crazy. Maybe bitcoin is money or can be money. Not in the sense that there is a low-probability chance—one that you cannot explain. But instead, in a logical way that allows you to actually see the path and explain to yourself *why* it may be possible.

Some people look at bitcoin and see it as the solution to money. Others think it's a delusion. Someone is right. It is either nothing or a masterpiece. By building a framework to think about bitcoin as money through logic and reason, an individual will typically connect with a particular principle or life experience that triggers an idea, like a flash in the brain connecting many dots simultaneously. It may be fleeting, but that moment is the most critical point on your journey. It is when you really *see* bitcoin for the first time. I describe it as a silhouette emerging from the fog. At first, you can see an outline, but the picture is not yet in focus. Also, it was just an idea that opened up the possibility in your mind. The proof is being able to consistently get back to that same idea through reason and logic. That is the only way to test its objectivity and truth. If you cannot return to the same conclusion consistently, it is likely not an objective truth.

Many questions will remain, but from the point of *maybe*, bitcoin will start to become intuitive and then over time, it will become hyper-intuitive.

My goal is to get you to the point where bitcoin starts to become intuitive as money, which depends on your ability to consistently arrive back at that conclusion. This book will lay the foundation to open up the possibility in your mind and reinforce it with logically ordered frameworks to understand the most fundamental questions about bitcoin, allowing you to be in a credible position to test each using your own reason and logic. *Gradually, Then Suddenly* is just a roadmap. By providing my reason and logic, I hope to accelerate the path of others, but importantly, my goal is not to convince. If you approach each essay as a construction of logical arguments and then challenge the validity of the components, that is the path to forming your own conclusions without relying on the opinions of others.

Over time, as questions arise, you will not need to reference any book but instead will reason through the questions with your own mental framework. There are no guarantees in life, but I expect you will come to the same conclusion that I did—that bitcoin obsoletes all other money. At the very least, you will have the benefit of a perspective that one would need to accept in order to come to similar conclusions. Understanding bitcoin is a personal journey. I have provided my explanation in the pages to follow. Only you can inform yours.

Synopses of Individual Essays

Part I – The Fundamentals

Bitcoin Obsoletes All Other Money | *First Principles of Money*

The hardest thing to understand about bitcoin starts with the question “what is money?” Money is not a collective hallucination nor a belief system. Money is a very basic necessity, which humans need to facilitate and scale trade. Economic systems converge on a single form of money due to the intersubjective problem of trade, and convergence on a particular medium is dictated by objective reasons and properties. The world is converging on bitcoin as money because it is finitely scarce, it is capable of being divided and aggregated into

small and large units, and it is capable of being transferred over a communication channel. In the competition of money, everything is always relative (A vs. B), and there is no second best. If money converges to one and bitcoin is finitely scarce, practically everyone in the world will adopt it as money.

Bitcoin, Not Blockchain | *A Foundation to Eliminate the Noise*

Many people have been sold a bill of goods that blockchain is a technology—believing blockchain to be more relevant than bitcoin. This essay debunks that. The concept of a blockchain was one piece of a larger puzzle specifically introduced in bitcoin for the purpose of ordering and validating financial transactions without the need to trust a third party. This piece explains why a blockchain is only viable in the application of money and because money converges to one, why only one blockchain is viable. There is no utility in a blockchain beyond its function in bitcoin for very fundamental reasons, and humans only need one form of money. Grasping the fundamental concept of what a “blockchain” is and why it is relevant to bitcoin is the starting point to drowning out the noise, when considered in the broader context of money.

Bitcoin Is Not Backed by Nothing | *What Secures Bitcoin's Fixed Supply*

But bitcoin isn't backed by anything while the dollar is backed by the full faith and credit of the US government, right? Wrong. Every fiat currency that has ever failed and hyperinflated has been controlled by a government, with both the ability to tax and a military. The dollar's origin as money began as a paper note convertible to physical gold. The dollar has no inherent monetary properties, and the same properties that allowed gold to emerge as money both exist in, and have been perfected through, bitcoin. The most important of these properties is scarcity. Bitcoin is finite in supply, and there are three primary pillars that secure bitcoin's fixed supply: mining, nodes, and private keys. How these work independently and together is critical to an understanding of the credibility of bitcoin's fixed supply and its position relative to the dollar.

Bitcoin Is Antifragile | *Gaining Strength through Adversity*

Bitcoin is often perceived as fragile or lacking permanence. However, rather than simply being resilient, antifragile systems become stronger when exposed to volatility, stressors, and error. The dollar becomes weaker when exposed to stress and volatility. Bitcoin is the opposite. The market constantly learns through trial and error. Moral hazard is eliminated and the cost of individual errors can never be socialized. Individual participants either adapt or die, but as a system, bitcoin gains strength in the face of adversity because it is decentralized at every layer and there are no single points of failure. As threats are immunized, the system becomes even more resistant to future attack. The antifragile nature of bitcoin ensures its permanence and serves as an important baseline to evaluate bitcoin's viability as money over the long term.

Bitcoin Is the Great Definancialization | *Implications and Consequences*

Modern money is engineered by central banks to lose value, and economies all over the world have become increasingly financialized as a direct result. Rather than simply being able to save, individuals are forced to put savings at constant risk through investments in financial assets in an attempt to offset or outpace inflation. What people really need is just a better form of money that will preserve value into the future. As knowledge distributes, individuals will increasingly opt for the simplicity of bitcoin as a saving mechanism over the complexity and risk of financial investing. The economy will definancialize through this process. More people will have savings, and greater economic stability will follow. There is a paradigm shift underway, and the only way to understand or explain the implications is through the incentives of money.

Part II – Common Misconceptions**Bitcoin Cannot Be Copied | *Finite Scarcity Only Happens Once***

When people begin to understand the significance of bitcoin's fixed supply, the question often arises, "why can't it just be copied?" Or improved and outcompeted. Bitcoin has been functionally copied thousands of times,

but none has ever come close to outcompeting it. Why? And will that ever change? The answer is anchored to the fundamentals of money. Money converges to one common medium due to the intersubjective nature of trade. Everyone is incentivized to adopt the best form of money, and in the end, that is the one that is hardest to produce. Scarcity is the foundation and bitcoin is finitely scarce. If bitcoin does have a credibly fixed supply and if money converges to one, it can never be copied and outcompeted for the reason that it already exists and can be adopted by anyone over inferior forms of money.

Bitcoin Is Not Too Volatile | *Volatility Does Not Prevent Adoption*

Bitcoin is volatile and that seems to fundamentally contradict common notions of money. The fact that bitcoin is volatile should prevent it from being money for the very reason that it is volatile, right? Bitcoin has existed for over fourteen years and adoption continues to grow. The better question is “why does volatility not prevent adoption of bitcoin as money?” Bitcoin has proven to be an exceptional store of value over time, which is fundamental to the function of money. While modern money is less volatile day to day, it loses value over time. Bitcoin may be volatile day to day, but it stores value over time. And its present volatility is also muted by exposure to other assets (i.e., diversification). Stability in bitcoin will emerge as a function of mass adoption, and the properties that allow bitcoin to store value over time—namely its fixed supply—drives adoption.

Bitcoin Does Not Waste Energy | *Scarcity Requires Real-World Cost*

All value in bitcoin is derived from the fact that there will only ever be 21 million. The foundation of bitcoin’s value proposition as money does not happen by magic either. Instead, its fixed supply is secured by real-world energy resources. Anyone who does not understand why bitcoin is valuable could never justify the cost and reasonably might believe its energy use is wasteful. However, money coordinates all other economic activity, including the fulfillment of energy. Without money and energy, reliable access to

power, water, food, healthcare and other daily essentials would not be possible. Everything of value comes with a cost, and there is no more important use for energy than securing the bitcoin network because it provides a sound form of money for the entire world to use, which will ultimately ensure all other demand for energy can be fulfilled via trade.

Bitcoin Is Not Too Slow | *A Fixed Supply Is the Zero to One Innovation*

The criticism that bitcoin is too slow typically comes from people trying to create a copy of bitcoin, who are really just searching for an excuse to print their own money. Its origin stems from the fact that bitcoin has a limited transaction capacity and transactions (technically blocks) are processed for final settlement on average every ten minutes. In reality, bitcoin's *0 to 1* innovation is finite scarcity—a fixed supply. A final settlement layer with a limited capacity combined with ten-minute block intervals are both part and parcel to the intricate puzzle that allows bitcoin to enforce its fixed supply. How bitcoin increases transaction volume and speed is a *1 to n* problem of scaling globally, and infrastructure is actively being developed to do just that. If human ingenuity could solve for finite scarcity, every other problem is pedestrian.

Bitcoin Is Not for Criminals | *Censorship Resistance Is All or Nothing*

For people who cannot gather why anyone would use bitcoin, the logical explanation becomes that it must be for some criminal or illicit purpose. If not, why else? Without doubt, bitcoin is inevitably used by criminals today. However, if bitcoin *works* for criminals, it would just establish that bitcoin is functional as money for the entire world. Bitcoin is viable as money because of its fixed supply, which is credibly enforced because bitcoin is decentralized and resistant to censorship. If it were possible to censor criminal activity or even a single transaction, it would establish that bitcoin is not sufficiently decentralized to be resistant to other forms of censorship, which would put everything at risk, including bitcoin's fixed supply. For bitcoin to be functional as money at all, it must be functional for everyone.

Bitcoin Cannot Be Banned | *A Currency System beyond Governments*

The idea that bitcoin will be banned is one of the later stages of denial on the path to adoption. It implies bitcoin being so successful as money that it threatens the government's monopoly on money. When that becomes apparent, then the government will ban it. Otherwise, there would be nothing to ban. Bitcoin is only viable as money because of its fixed supply, and if bitcoin can credibly enforce its fixed supply, it is path dependent on being resistant to all forms of censorship, including state attacks. China and India have both attempted to ban bitcoin, and it continues to function without interruption. Bitcoin exists beyond government, and the mechanisms that enforce its fixed supply also ensure that no government or group of state actors could prevent its use. Government attempts to ban bitcoin only cause broader adoption.

Bitcoin Is Not a Pyramid Scheme | *Supply Constraints and Demand*

A pyramid scheme is loosely defined as an investment fraud in which new-participant fees are used to pay money to existing participants for recruiting new members. With a pyramid scheme, there is always a company purporting to offer a good or service, but in reality, there is not actual demand for the service, and functionally, the supply is unlimited relative to its demand. Bitcoin is not a company. It does not have a CEO. It has no employees, and its supply is finitely scarce. No matter how many people adopt it, there will only ever be 21 million bitcoin. Bitcoin's utility is as money. It has a market because it solves a problem inherent in modern money. Whereas in a pyramid scheme there is not real demand for the product, everyone in the world needs money, and bitcoin represents a form of money that cannot be printed by anyone.

Part III – Bitcoin vs. the Dollar**Bitcoin Fixes This | *The Solution to Money Printing***

There is a saying popular among bitcoiners that *bitcoin fixes this*, which is generally applied to just about anything in the world. Expanding wealth gaps, endless global war, a diabetes epidemic and virtually every other

real-world problem. Money serves as the foundation of the economic system because money facilitates trade. If the monetary system is broken, it is logical that many derivative problems would be created downstream as a consequence. However, what bitcoin fixes at a first-order level is the money and the problem of printing money. The term “quantitative easing” is used in mainstream economic and finance circles quite a bit. *Gradually, Then Suddenly* references it frequently. But what is quantitative easing? It is the modern digital equivalent of money printing, and bitcoin eliminates the ability to print money entirely, forever and for everyone.

Bitcoin Is a Rally Cry | *The Only Viable Path to Opt Out*

The instability in the banking system that became evident during the 2008 financial crisis reappeared in 2019. In response, the Federal Reserve began introducing emergency liquidity to financial markets and reduced interest rates back to zero in an attempt to create stability. The efforts proved unsuccessful, and financial markets functionally collapsed in early 2020 as a dollar liquidity crisis developed rapidly. Not immune, bitcoin crashed by 50% in a single day, down to \$4,000. To stem the crisis, the Fed announced plans to print an unlimited amount of money. Printing money never ends, and it is the definition of insanity. Despite its volatility, bitcoin is the solution to the dollar. The fragility and instability in the global economy is caused by central banks, and bitcoin is a rallying cry for anyone who wants to opt out of the madness.

Bitcoin Is Common Sense | *Simplicity vs. Complexity*

The Fed ultimately created \$3 trillion dollars over the months following its announcement in March 2020 that it would launch an unlimited campaign to print money via quantitative easing. In *Common Sense*, a famous pamphlet published anonymously on January 10, 1776, at the beginning of the American Revolution, Thomas Paine explained that *time makes more converts than reason*. Bitcoin is often described as an IQ test, but it is really just a “common sense” test. Bitcoin can be as simple or complicated as you wish

to make it. The Federal Reserve continues to print trillions upon trillions of dollars, and bitcoin cannot be printed at all. There will only ever be 21 million and at its highest level, the competition between these two forms of money comes down to supply. One is infinite and the other is finite. Bitcoin is common sense.

Bitcoin Is One for All | *The Most Equitable System for Everyone*

There is a growing consensus that massive and expanding wealth gaps are a problem. No one knows how to fix it, but politicians from all sides of the aisle continue to make promises, which can never be kept and rarely fail to sow further division. Thankfully, the problem is not political in nature. The unsustainable gaps in wealth are a function of a broken monetary system. Economic inequality itself is perfectly consistent with balance. However, the dollar system creates inequities that would otherwise not exist. By printing money, the Fed actively causes imbalances to be sustained and exacerbated. While many people believe bitcoin is not suitable for those on the lower end of the economic spectrum, it solves a problem for everyone regardless of wealth and will help restore balance. Bitcoin is one currency for all to use.

Historical Reference Index

Gradually, Then Suddenly Edition	Original Author Date	Dollars in Circulation	Dollar Price			
			Bitcoin	Oil	Gold	S&P 500
Bitcoin Is Money	Jul 26, 2019	\$3.85tn	\$9,870	\$56	\$1,418	\$3,026
Bitcoin Cannot Be Copied	Aug 02, 2019	\$3.83tn	\$10,518	\$56	\$1,446	\$2,932
Bitcoin Is Not Too Volatile	Aug 09, 2019	\$3.83tn	\$11,863	\$54	\$1,497	\$2,919
Bitcoin Does Not Waste Energy	Aug 16, 2019	\$3.83tn	\$10,374	\$55	\$1,513	\$2,889
Bitcoin Is Not Too Slow	Aug 23, 2019	\$3.81tn	\$10,408	\$54	\$1,527	\$2,847
Bitcoin Fixes This	Aug 30, 2019	\$3.81tn	\$9,598	\$55	\$1,519	\$2,878
Bitcoin, Not Blockchain	Sep 06, 2019	\$3.81tn	\$10,353	\$57	\$1,506	\$2,979
Bitcoin Is Not Backed by Nothing	Sep 27, 2019	\$3.91tn	\$8,252	\$56	\$1,499	\$2,961
Bitcoin Is Not a Pyramid Scheme	Oct 18, 2019	\$4.01tn	\$7,973	\$54	\$1,488	\$2,986
Bitcoin Cannot Be Banned	Nov 08, 2019	\$4.09tn	\$8,805	\$57	\$1,461	\$3,093
Bitcoin Is Not for Criminals	Nov 29, 2019	\$4.10tn	\$7,761	\$55	\$1,466	\$3,141
Bitcoin Obsoletes All Other Money	Jan 24, 2020	\$4.19tn	\$8,445	\$54	\$1,571	\$3,295
Bitcoin Is a Rally Cry	Mar 26, 2020	\$5.03tn	\$6,716	\$23	\$1,650	\$2,630
Bitcoin Is Common Sense	May 01, 2020	\$6.71tn	\$8,864	\$20	\$1,695	\$2,830
Bitcoin Is Antifragile	Jun 12, 2020	\$7.22tn	\$9,480	\$36	\$1,729	\$3,041
Bitcoin Is One for All	Aug 27, 2020	\$7.04tn	\$11,323	\$43	\$1,921	\$3,484
Bitcoin Is the Great Definancialization	Dec 23, 2020	\$7.45tn	\$23,241	\$48	\$1,875	\$3,690
As of Publication	May 03, 2023	\$8.61tn	\$28,954	\$68	\$2,014	\$4,091

Source: Federal Reserve Economic Data, Yahoo Finance

PART I

The Fundamentals

CHAPTER ONE

Bitcoin Obsoletes All Other Money

(Originally published on 24 January 2020)

One Thousand Possibilities, 999 Problems

There are two rules that never seem to fail when it comes to bitcoin adoption. Everyone always feels late, and everyone always wishes they had bought more bitcoin. While there are exceptions to every rule, bitcoin has an uncanny ability to screw with the human psyche. It turns out that 21 million as a nominal currency supply is a very small number. And it is a number that becomes ever smaller as more individuals adopt bitcoin, which occurs as more people figure out that bitcoin's fixed supply is credibly enforced and that economic systems converge on a single form of money.

Demand for bitcoin is driven by the credibility of its monetary properties and the convergent nature of money. As more people adopt bitcoin, there is increasing competition for a resource fixed in supply, which causes bitcoin to become more and more scarce. As it does, bitcoin becomes more valuable as a monetary medium. While this becomes evident the further one travels down the bitcoin rabbit hole, it is not uncommon for individuals on the periphery to be overwhelmed by the sheer number of cryptocurrencies. Sure, bitcoin is in the "lead" today, but there are thousands of others. How do you know bitcoin is not Myspace? How can you be sure that something new doesn't overtake bitcoin?

It may sound crazy to believe that bitcoin will become the dominant global currency if you're evaluating the possibility from a top-down,

probability-weighted perspective. Today, bitcoin is one of more than a thousand digital currencies that all look the same on the surface. Its current purchasing power of \$150 billion (as of the time of writing), is a drop in the bucket compared to the global financial system, which supports \$250 trillion of debt. Gold alone has a purchasing power of \$8 trillion (50 times the size of bitcoin). What are the chances that an eleven-year-old internet sensation rises from the ashes of the 2008 financial crisis and goes from nothing to becoming the dominant global currency? The idea sounds laughable. Or at the very least, it appears to be too low of a probability to warrant consideration.

Evaluating one thousand possibilities in the hope of coming to the right solution may not be practical or possible. However, when taking a bottom-up approach and developing conviction around a few foundational principles, it becomes more practical to arrive at a coherent answer. Combined, the following foundational principles bring simplicity and clarity to what may have once seemed too complex to possibly discern.

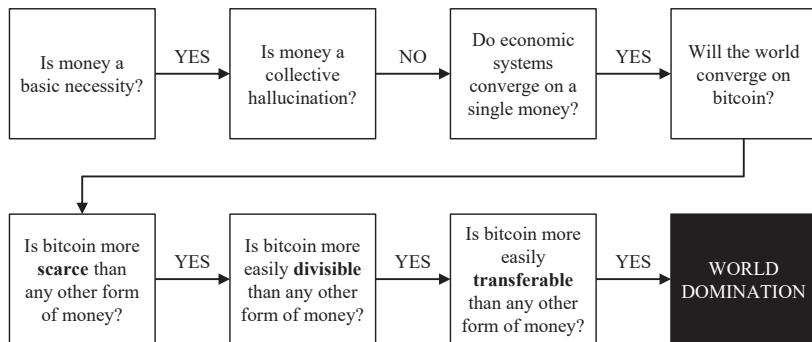


FIGURE I.1

This roadmap is critical and will help you cut through the noise and focus on what really matters. Individuals may come to different conclusions concerning any of these questions, but this is the path to consider when attempting to understand why bitcoin consistently outcompetes all other currencies (and whether it will continue to do so). Money is a basic

necessity, but it is not a collective hallucination or a shared belief system. Individuals adopt bitcoin because it possesses unique properties that make it superior as a form of money relative to all other forms of money. Because money solves an intersubjective problem, monetary systems tend to converge on a single medium. Or rather, economic systems naturally emerge from the common use of a single medium due to the function of money. The properties inherent in bitcoin are causing the market to converge on it as a tool to communicate and measure value because it represents a step-function change improvement over any other monetary medium. If anyone comes to the fundamental conclusion that money is a basic necessity and that monetary systems naturally converge, the question then centers on whether bitcoin is optimized to fulfill the monetary function better than any other medium.

Money Is a Necessity

Civilization as we know it would not exist without money. There would be no airplanes, cars, or iPhones, and the ability to fulfill very basic necessities would become materially impaired. Millions of people could not peacefully inhabit a single city, state, or country without the coordination function that money enables. Money is the economic good that allows for food to reliably show up on grocery store shelves, gas to be at the gas station, electricity to be supplied to power homes, and clean water to be abundant. It is money that makes the world turn, and it would not turn in the way that most have taken for granted if not for the function of money. Money serves a massively underappreciated function and one that is poorly understood because it is generally not consciously considered. In the developed world, reliable money is taken as given. So too are the basic necessities delivered through the coordination function of money.

Consider, for example, a local grocery store and the range of choice that converges in a single place. The number of individual contributions and skills required to make that happen is mind-boggling, from the coordination of the

store itself to the individual packaging, to the technology providers, to the logistics networks, to the transportation networks, to the payments systems, and right down to each item of food. Then, as a derivative, consider all the unique inputs that go into each item on the shelf. The grocery store is just the fulfillment side. The production of each input has its own diverse supply chain. And it is just one modern marvel. Deconstructing the inputs of a modern telecom network, energy grid, or water treatment and waste management system is similarly complex. Each network and the participants therein rely on the others. Food producers depend on individuals who help fulfill energy demand, telecom services, logistics, and clean water, among others—and vice versa. Practically all networks are connected, and it is all made possible through the coordination function of money. Everyone can contribute their skills based on their own interests and preferences, receive money in return for value delivered today, and then use that same money to acquire the specialized value created by others in the future.

None of this happens by chance. Some not-so-rigorous thinkers suggest that money is either a collective hallucination or derives its value from the government. In reality, money is a tool invented by man to satisfy a very specific market need. Money helps facilitate trade by acting as an intermediary between a series of present and future exchanges. Without any conscious control or direction, market participants evaluate various goods and converge on the tool best suited to convert present value for future value. Whereas individual consumption preferences vary from person to person and change constantly, the need for exchange is practically universal, and the function is distinctly uniform. For every individual, money allows value produced in the present to be converted into consumption in the future. The value one places on a home, a car, food, leisure, etc. naturally changes over time and varies among individuals. But the need to consume, exchange value, and communicate preferences does not change and applies to all individuals on an intersubjective basis.

Money exists to communicate these preferences and, ultimately, to exchange value. But recognizing that all value is subjective (and not intrinsic),

money forms the baseline to establish an expression of value and, more importantly, relative value. Money represents the collective recognition that everyone benefits from the existence of a common language to communicate individual preferences. The function of money aggregates and measures the preferences of all individuals within an economy at any point in time, and it would be practically impossible—or at the very least, extremely inefficient—to communicate or quantify value if not for a common constant upon which everyone could agree. Think of money as the constant against which to measure all other goods. If it did not exist, everyone would be at a practical standstill, unable to agree on the value of anything. Comparing against a single constant makes it more practical to discern the relative value of two other goods. There are millions of goods and services produced by billions of individuals, all with unique preferences. Through convergence on a single form of money, a price system ultimately emerges, without which standardized value could not be quantified. By measuring and expressing the value of all goods in a common intermediary (money), it then becomes possible to discern how much one good (or resource) is valued relative to any other.

Without a common currency, there would be no concept of price. And without the concept of price, it would be impossible to do any range of economic calculations. The ability to perform economic calculations allows individuals to take independent actions, relying on the information communicated through a price system, to best satisfy their own needs by understanding the needs of others. It is a price system that allows supply and demand structures to form. And a price system is ultimately a necessity because it provides for the communication of information, without which the fulfillment of basic needs would not be possible. Imagine if nothing you consumed had a discernible price. How would you know what you needed to produce in order to obtain the goods you value in exchange? Recognize that your own conception of the value you produce, and the very existence of goods and services produced by others, would not be available if not for some expression of price existing. It becomes circular, but money is the good that allows the underlying structures of an economy to form through the

price system. While often lamented as the root of all evil, money may just be the greatest accidental invention ever created and one that could not have emerged by conscious control.

Factors Determining Price & Relative Price under a Constant Money Supply

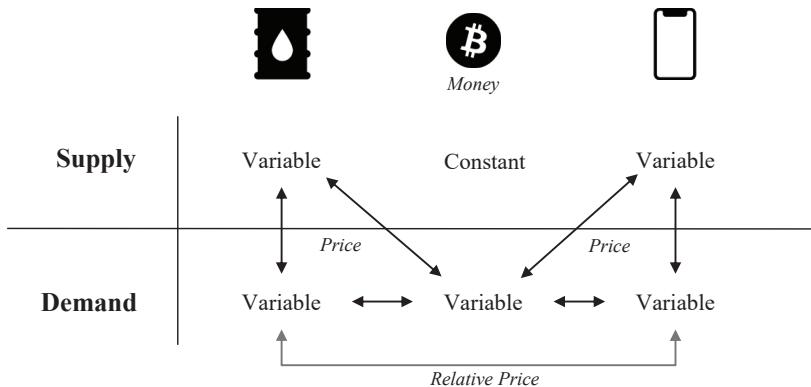


FIGURE 1.2

I have deliberately used the word “marvel” to shock the reader out of the complacency with which we often take the working of this mechanism for granted. I am convinced that if it were the result of deliberate human design, and if the people guided by the price changes understood that their decisions have significance far beyond their immediate aim, this mechanism would have been acclaimed as one of the greatest triumphs of the human mind. Its misfortune is the double one that it is not the product of human design and that the people guided by it usually do not know why they are made to do what they do.

—Friedrich A. Hayek²

2. Friedrich A. Hayek, “The Use of Knowledge in Society,” *American Economic Review* 35, no. 4 (September 1945): 527.

Economic Systems Converge on a Single Form of Money

As a starting point, accept that two facts are true—the world previously converged on one form of money (i.e., the Gold Standard), and while there may be a few hundred fiat currencies in existence globally, virtually every individual and business in the world only transacts in *one* form of money on a daily basis. Neither is a coincidence, and both are deeply rooted in the nature of money. Even still, the phenomenon is not immediately intuitive, and late-stage Silicon Valley thinking has many people believing that hundreds, if not thousands, of currencies may exist in the future. The machines are going to do all the calculations! Artificial intelligence and quantum computing will handle it. An intellectually “safe” view to hold is that 95% of cryptocurrencies will probably fail, but there are some “interesting” projects. The logic mimics venture capital investing—it is inherently difficult to know which will succeed, and while most will fail, the ones that win will win big. At least, this is what most of Silicon Valley would have you believe because it is a defensible parallel to the historical experiences of investing in early-stage venture companies. In reality, it is a blanket hedge lacking in first principles. It also applies a familiar formula to an entirely different class of problem.

While it may seem logical to form a mental framework around bitcoin in relation to the rhyming history of technology startups, there can be no comparison whatsoever. Bitcoin is money, not a company. It would be illogical to assume competition between monetary mediums would follow a similar pattern to that of companies. Companies compete in a capital formation and capital accumulation arms race. To do so, they need money to coordinate economic activity. How do they get money? By using money to coordinate the production of goods and services and by selling the output for more money (profit). In essence, companies compete for the same pool of money in order to accumulate capital. Money is the tool that makes the wheel go round. It simply would not be possible to coordinate all the individual skills necessary to produce goods and services derived from complex

modern supply chains without money. It would also not be possible if not for a large group of people accepting a common form of money.

Having a single medium of exchange allows the size of the economy to grow as large as the number of people willing to use that medium of exchange. The larger the size of the economy, the larger the opportunities for gains from exchange and specialization, and perhaps more significantly, the longer and more sophisticated the structure of production can become.

—Saifedean Ammous³

Value is created by individuals through the fulfillment of goods and services. However, the communication of this value is not direct. Instead, it is communicated through money as an intermediary. Money provides the baseline to express the very concept of value. Every time an individual converts goods or services into money, a price is determined or changed, and information is communicated. Price is ultimately the information, and money is the medium through which price is communicated and value is exchanged. While all other goods are non-fungible and variable, money is a utility because it provides a single, fungible constant that allows for the measure and exchange of value.

In the production supply chain, money serves a distinct function from all other individual goods or services. It is the distinction between the fulfillment of preferences (production of goods and services) and the coordination of preferences (money). The fulfillment of preferences is dependent on the coordination of preferences, and the coordination of preferences is dependent on a price system, which can only form as a derivative of mass convergence on a single monetary medium. Without a pricing system, division of labor would not exist, at least not to the extent necessary to allow for the functioning of complex supply chains. This is the root-level principle most miss when contemplating a world of many currencies. Any pricing

3. Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Wiley, 2018), 8.

system derives from a single currency. Convergence is a precursor. The concept of price (and relative price) would not exist if not for a critical mass of individuals producing a diverse range of goods and services and communicating the value of those goods and services through a common medium. As a result, it may be more accurate to say that economic systems emerge from the common use of a single monetary medium rather than *converge* on one. Individuals converge on a single form of money, and the output is an economic system.

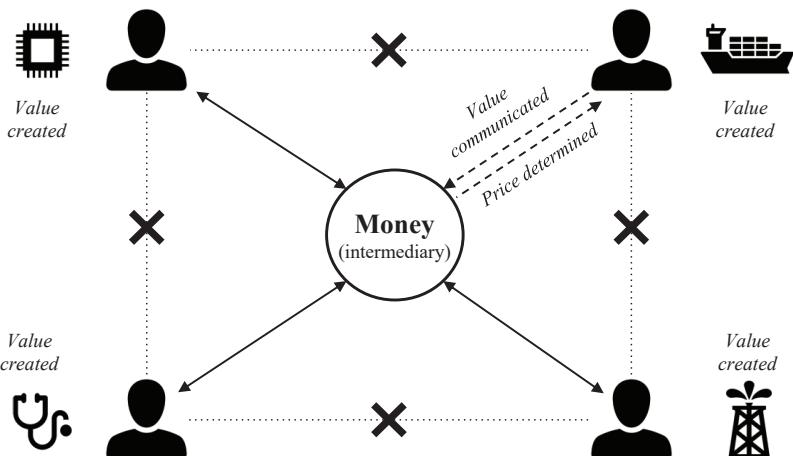


FIGURE 1.3

Whereas the value of all other goods and services is in their consumption, the value of money lies in the utility of exchange. Exchange is the good an individual purchases when choosing to convert value (the subjective output of time, labor, and physical capital) into a monetary good. Individual consumption preferences are unique, but money serves one singular function for all market participants: to bridge the present to the future (whether it be for a day, week, year, or longer). In any exchange of present value, some time continuum exists until a future exchange. At the point of exchange, each individual must decide which monetary good will best serve the function of preserving value created in the present into the future. A

or B? While an individual can choose to hold one or multiple currencies, one form of money will preserve future purchasing power better than the others. Everyone intuitively understands this and makes a decision based on the inherent properties of one medium relative to another. When deciding which monetary good to use, the preference of one individual is impacted by the preference of others, but each individual is making an independent evaluation discerning the relative strengths of multiple monetary goods. I must have the form of money you are willing to accept in order for us to trade and the identical problem extends out to every single person in an economy. It is not a coincidence that the market converges on a single medium because each individual is attempting to solve the same problem of future exchange—an intersubjective problem dependent upon the preference of others.

The ultimate goal is to reach a consensus so each individual can communicate and exchange value with the widest and most relevant set of trading partners. It is an objective evaluation of tangible goods based on an intersubjective need. The whole point is to find the one good that everyone can agree is (1) a relative constant, (2) measurable, and (3) functional in exchange. The existence of a constant creates order where none existed previously, but that constant must also be functional as both a measurement tool and a means of exchange. It is the combination of these characteristics—often described as aggregating the properties of scarcity, durability, fungibility, divisibility, and transferability—that is unique to money. Very few goods possess all of these properties, and every good is unique, with inherent properties that cause each to be better or worse in fulfilling certain functions within an economy. A is always different than B, and the combination of properties required for a good to be viable as money is so rare that the distinction from one to another is never marginal.

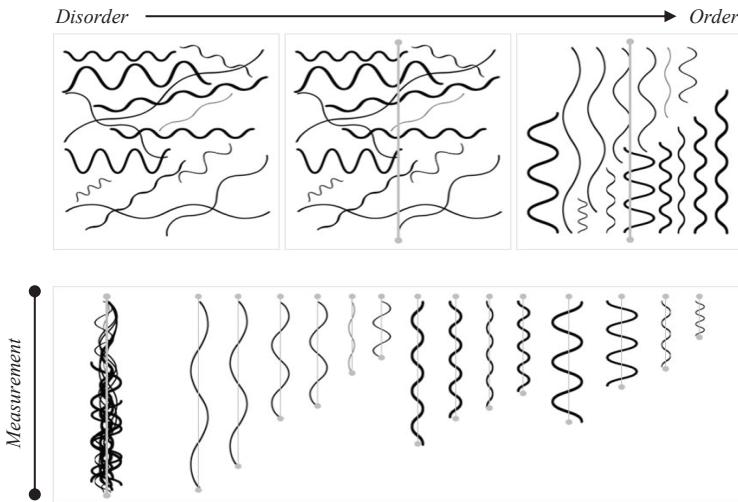


FIGURE 1.4

On a more practical level, everyone agrees on a single monetary good through which to express value because it is in their individual and collective interest to do so. That is the problem itself—how to communicate and trade value with other market participants. It would be counterproductive to the entire exercise if a consensus were not formed. However, a consensus is not reached randomly. The properties inherent to a specific monetary good cause a convergence and consensus to emerge. The imagined world of thousands of currencies is blind to these fundamental first principles. A critical mass of individuals converging on a common medium is the input required to ascertain the information and benefit that is actually desired: a price system along with the ability to trade. And the value of a common medium only increases as more and more people converge on it as a tool to facilitate exchanges. The fundamental reason is that as more individuals converge on a single medium, the medium accumulates more information and greater utility—more prices and more opportunities to trade.

Think of each individual as a potential trading partner. As individuals adopt the common medium as a standard of value, all existing participants

in the monetary network gain new trading partners, as do those joining the network. There is mutual benefit to existing holders of the currency and new adopters that comes from increased adoption. As the monetary network expands, the range of choice also expands as more goods come to be denominated in and traded for the common medium of exchange. More prices exist, which enables more relative prices as a result. More information is aggregated into the common medium, which can then be relied upon by all individuals within the network (and the network as a whole) to better coordinate resources and respond to changing preferences via trade. The constant becomes more valuable and inherently more reliable as it communicates more information about more goods produced by more individuals. The more variable information communicated through the constant, the more constant it becomes relative to all other goods and services in aggregate.

Network Adoption and Possible Network Connections

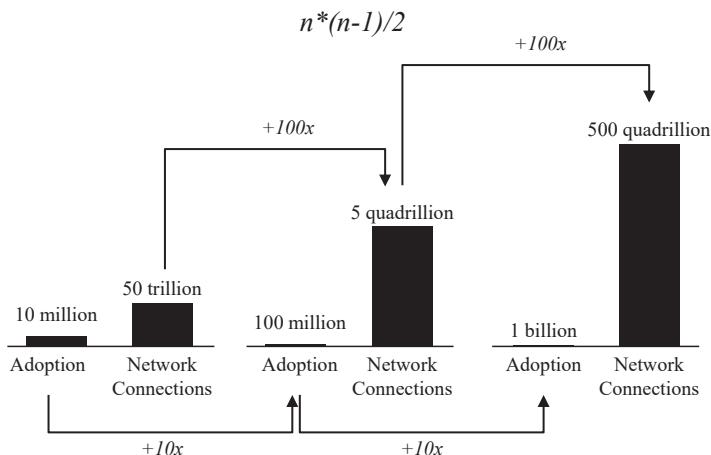


FIGURE 1.5

As the adoption of a monetary network increases by an order of magnitude (10x), possible network connections increase by two orders of magnitude (100x). While this helps demonstrate the mutual benefit of adoption, it also highlights the consequence of converting value into a

smaller monetary network. A network one-tenth the size has only 1% of the number of potential connections. Not every network distribution is equal, but a larger monetary network translates to a more reliable constant to communicate information—greater density, more relevant information, and ultimately, a broader range of choice. The size of a monetary network and its expected growth become critical components of the intersubjective A/B test when individuals are determining which form of money to use. While the number of social relationships an individual can maintain is inherently limited, the same limits do not apply to monetary networks. Money is what allows humans to break from the constraints of Dunbar's number (the theorized maximum number of interpersonal relationships one can reasonably maintain). A monetary network allows millions (if not billions) of people unknown to each other to contribute value at endpoints in the network, with relatively few direct connections needed.

Monetary networks ultimately accumulate the value of all other networks because all other network effects would not exist without a monetary network. Complex networks cannot form without a common currency to coordinate the economic inputs necessary to kick-start the positive feedback loops of price. A common currency is the foundation of any monetary network, allowing other value networks to form. It provides the common language to communicate value, leading to trade and specialization, and organically creating the ability to expand the use of resources beyond the reach of "conscious control" (to borrow from Hayek). When contemplating the network effects of a social network, logistics network, telecom network, energy grid, etc., add them all together—that is the value of a monetary network. It not only provides the foundation for all other value networks to form, but the currency pays for access to all derivative networks within the monetary network. The existence of a common currency is the engine and the oil.

Admittedly, multiple currencies—the dollar, euro, yen, pound, franc, yuan, ruble, lira, peso, etc.—all coexist today. But this is not a natural phenomenon inherent to an open, global economy. Fiat currencies emerged as a

fractional representation of gold, which the world had previously converged upon as a monetary standard. None would subsist without the forces of government intervention, nor would any fiat currency have ever emerged if not for the prior existence (and limitations) of gold—or the backing of another commodity metal—as a monetary medium. While modern monetary theorists and gold bugs alike will never admit it, the calamity that is all fiat systems is nothing more than the manifestation of gold's failure as a monetary medium. It is a dead man walking. Following the formal abandonment of the gold standard in 1971, the subsistence of jurisdictional fiat systems merely represents a transient departure from free-market monetary forces. Modern fiat systems have only survived this long because a solution to the very problem created by fiat currencies did not yet exist. Bitcoin is that solution, and since its creation, individuals have been converging on it as a new monetary standard. It is a trend that will only continue as knowledge naturally distributes.

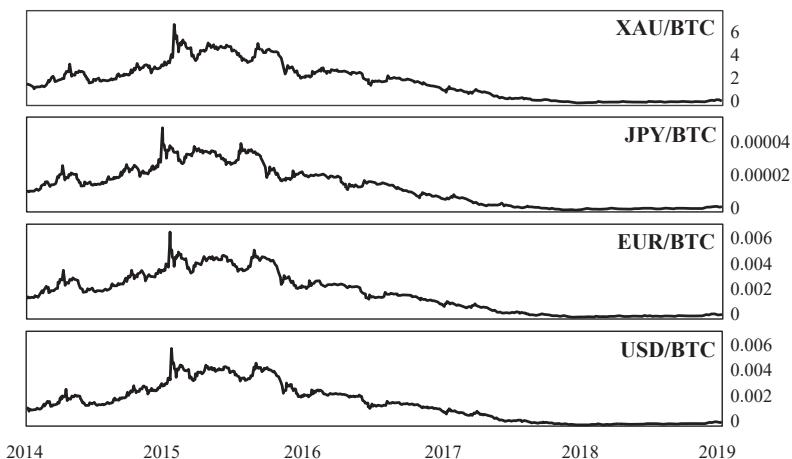


FIGURE I.6

Source: pricedinbitcoin21.com

All Roads Converge on Bitcoin

The Greatest Constant—Finite Scarcity

The market is converging on bitcoin over time, and its value continues to increase because it provides a constant—a fixed supply not susceptible to change—that is superior to all other forms of money. Bitcoin has an optimal monetary policy, and that policy is credibly enforced on a decentralized basis. Only 21 million bitcoin will ever exist—a fixed maximum supply that is enforced by a network consensus mechanism on a decentralized basis, eliminating the element of trust entirely. No one trusts anyone, and everyone enforces the rules independently. As an aggregate of these two functions—an optimal monetary policy that is credibly enforced without trust—bitcoin is becoming the rarest form of money that has ever existed.

Finite scarcity is a property no other form of money has ever or will ever achieve, and demand for bitcoin is fundamentally driven by that scarcity. However, scarcity is a two-sided equation. A fixed supply may be the primary draw, but demand is a critical and often overlooked aspect of scarcity. Demand is what makes scarcity a utility as a constant in exchange. Bitcoin becomes increasingly scarce as a combined function of both increasing demand and a perfectly inelastic terminal supply. The scarcity of its fixed supply creates demand, but increasing demand creates greater scarcity. It sounds circular because it is. If there were 21 million bitcoin and only one person valued them, there would be nothing scarce or useful about bitcoin. But if 100 million people valued bitcoin, 21 million would start becoming scarce. And if the network grew to one billion people, 21 million would become extremely scarce, and the constant that bitcoin provides would offer even greater utility in facilitating trade.

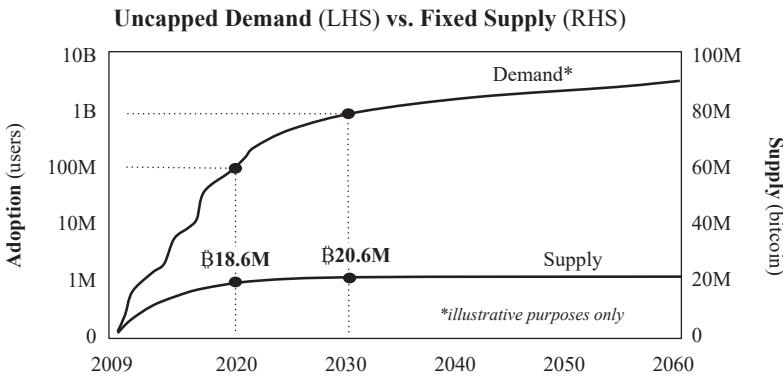


FIGURE 1.7

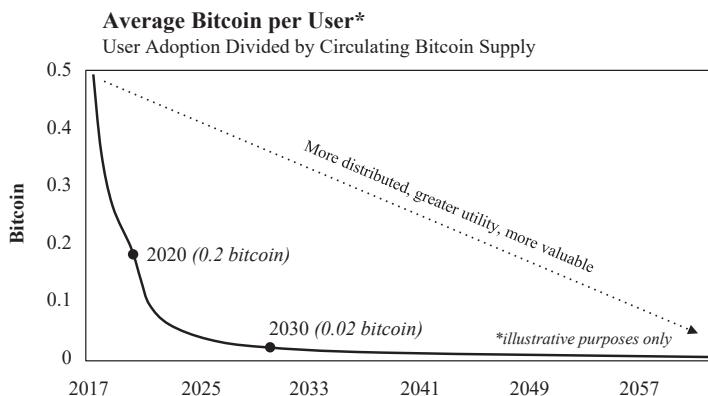


FIGURE 1.8

Increased demand combined with a fixed supply naturally results in bitcoin becoming more distributed. There is only so much to go around, and the pie ends up getting split up into smaller and smaller shares owned by more and more people. As more individuals value bitcoin, the network not only becomes a greater utility, but it also becomes more secure. It becomes a greater utility because more people are communicating in the same language of value and trading through a more reliable constant. And as more individuals participate in the network consensus mechanism, the entire system becomes more

resistant to corruption and ultimately more secure. Recognize that there is nothing about a software application or a “blockchain” that guarantees a fixed supply, and bitcoin’s supply schedule is not credible because software dictates it. Instead, 21 million is only credible because it is governed on a decentralized basis and by an ever-increasing number of network participants. The more decentralized bitcoin becomes, the more secure it is. As more individuals participate in consensus, 21 million becomes a more credibly fixed number. Similarly, bitcoin becomes a more reliable constant as each individual controls a smaller and smaller share over time. As adoption increases, security and utility work in lockstep. Consider the distribution and relative density of bitcoin adoption worldwide. As reach and density within each market spread, bitcoin’s constant hardens and becomes harder to change.

Global Bitcoin Node Distribution (Reachable)
Snapshot: November 2019



FIGURE 1.9
Source: Bitnodes.io

As individuals increasingly opt in, bitcoin’s terminal supply of 21 million becomes more and more credible. In the mind of those who adopt it, finite scarcity becomes what differentiates bitcoin from all other forms of money—both legacy currencies and competing cryptocurrencies alike. All other currencies either become centralized over time (e.g., the dollar, euro,

yen, gold) or were too centralized from the start (e.g., all other cryptocurrencies) to credibly compete with a fixed supply of 21 million. Centralization inherently creates the need to rely on trust, and trust puts the supply of any currency at risk. As history has shown, the desire and impulse to print money are far too great to resist, and an inflating currency supply ultimately impairs demand and marginalizes utility of the currency in the function of exchange. Whereas all other currencies depend on trust, bitcoin provides a trustless constant. Twenty-one million is only credible because bitcoin is decentralized, and bitcoin becomes increasingly decentralized over time. The best any other form of money could possibly do is match bitcoin. However, even that is not possible because individuals converge on a single form of money, and bitcoin has already beaten every other currency to the punch. Every other currency is ultimately competing against the ideal constant—one that is fixed, will not change, and does not rely on trust.

Currency Supply: Annual Rate of Change (2011–2019)



One of these things is not like the others.

FIGURE 1.10

Source: Federal Reserve Economic Data (FRED)

All forms of money compete with each other for every exchange. If an asset's primary (or sole) utility is the exchange for other goods and services, and if it does not have a claim on the income stream of a productive asset

such as a stock or bond, it must compete as a form of money. As a consequence, any such asset is directly competing with bitcoin for the exact same use case. And because bitcoin already exists and is finite, no other currency will ever provide a more reliable constant. Scarcity in bitcoin will also be perpetually reinforced on both the supply and demand side for the reason that individuals converge on a single form of money. At the same time, the opposite force will be in effect for all other currencies due to the reflexive nature of monetary competition. The distinction between two monetary goods is never marginal, and neither is the consequence of individual decisions to exchange in one medium rather than another. Money is an intersubjective problem, and opting in to one monetary medium explicitly means opting out of another, even if on a marginal basis with each trade or exchange. One currency gains value and utility at the direct expense of the other. As bitcoin becomes more scarce and more reliable as a constant, other currencies become less scarce and more variable (i.e., less stable and more volatile). Monetary competition is zero-sum, and relative scarcity, a dynamic function of supply and demand, creates the fundamental differentiation between two monetary mediums, which only increases and becomes more apparent over time.

But remember, scarcity for scarcity's sake is not the goal of any money. Instead, the money that provides the greatest constant will facilitate exchange most effectively. The monetary good with the greatest relative scarcity will best preserve value between present and future exchanges over time. The relative price and relative value of all other goods is the information desired from the coordination function of money, and in every exchange, each individual is incentivized to maximize present value into the future. Finite scarcity in bitcoin provides the greatest assurance that value exchanged in the present will be preserved into the future. As more and more individuals collectively identify that bitcoin is the monetary good with the greatest relative scarcity, stability in its price will become an emergent property.

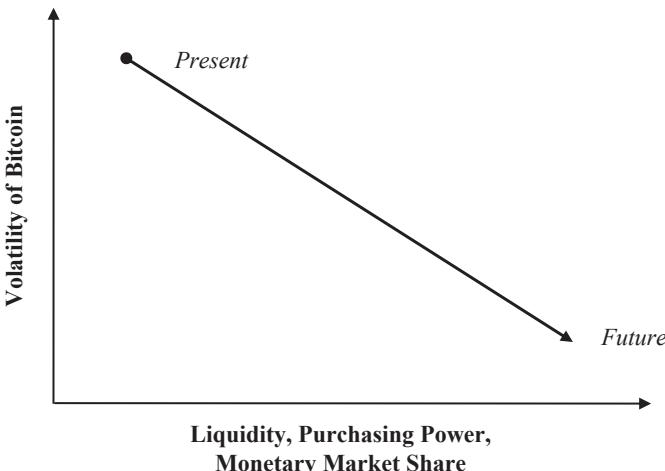


FIGURE 1.11

The Greatest Measurement Tool—Divisibility

While scarcity is the bedrock of a monetary good, not all scarce goods are functional as money. To effectively communicate value, a monetary good must be a relative constant, easy to measure, and functional in exchange—all three in aggregate. Naturally, goods that are easy to measure or otherwise serve as measurement tools are not necessarily effective in the exchange of value. A ruler may be an effective measurement tool, but rulers are not scarce, nor can they be easily divided or aggregated into larger and smaller units to facilitate exchange. A monetary good being scarce and measurable allows for the measurement of all other goods. However, the ability to easily subdivide and transfer a monetary unit provides practical utility in exchange, without which a particular good would not be used as a standard to measure *value*. Bitcoin combines finite scarcity with the ability to subdivide each whole unit down to eight decimal points (0.00000001 or one 100,000,000th of a bitcoin) and transfer any amount of value, however large or small. Just as scarcity for scarcity's sake is not necessarily valuable in the context of money, neither is the property of divisibility. It is the

combination that becomes valuable in the context of money, particularly when each subdivided unit is fungible (i.e., essentially interchangeable, with each part indistinguishable from another). These properties jointly allow bitcoin to be both a perfect constant and an effective measure of value to facilitate exchange.

In the code, one bitcoin is represented as 100,000,000 sub-units, with the smallest unit referred to as a satoshi (or sat for short). Technically, one bitcoin is 100,000,000 sats. While one bitcoin equates to approximately \$9,000 as of the time of writing, one satoshi equals one-twentieth of a penny. In essence, anyone can exchange any amount of value for bitcoin. Bitcoin, as with any money, is functional for one purpose, to store value between a series of exchanges. Receive bitcoin for value produced today, save, and spend bitcoin in the future in exchange for value produced by others. Bitcoin will perform the same function regardless of the amount. The practical consequence of divisibility is that bitcoin can measure any and all value, allowing it to support any and all adoption. Individuals produce a wide range of value, and divisibility allows all individuals to utilize bitcoin as a savings mechanism, whether it be to store \$50 or \$50,000 worth of value. For a monetary good to be an effective exchange tool, it must be able to measure the range of value produced by all individuals—something bitcoin does flawlessly. The ability to divide and transfer any amount of bitcoin makes it accessible to all individuals and, ultimately, all goods produced, regardless of how much value is attributable to each.

In the A/B test of monetary competition, if A>B, any amount of A will perform the function of money better than any amount of B. Over time, A will increase in purchasing power relative to B, whether for \$50 or \$50,000 worth of value. Never be confused by a list of cryptocurrencies trading on Coinbase that look like a better deal because the price is “cheap” whereas bitcoin appears “expensive.” Remember that bitcoin can be divided into smaller or larger units to store more or less value. One bitcoin is an inherently arbitrary unit, as is one unit of any currency. The market test is whether A is more functional as money than B. It is an intersubjective decision, and

while the market is communicating which network it believes performs the monetary function more effectively through price and value, network value is the output—not the input. The input is each individual evaluating the properties of the monetary good itself relative to others. If bitcoin is A in your evaluation, then there is no “too expensive.” Bitcoin may be overvalued or undervalued at any point in time, but each individual that adopts bitcoin increases the value of the network (recall the discussion on trading partners and network connections). And the ability to be divided easily into very small units allows a practically limitless number of individuals to convert and communicate value through the network. If A is greater than B, and if A can support unlimited adoption, it eventually obsoletes the need for network B entirely.

Network Value	\$100 billion	\$1 trillion	\$10 trillion
Nominal amount of bitcoin to send \$10,000	2.1 bitcoin	0.21 bitcoin	0.021 bitcoin
Maximum # of individuals capable of sending \$10,000 of bitcoin	10 million	100 million	1 billion

FIGURE 1.12

As individuals independently evaluate this A/B test, more people ultimately adopt bitcoin, and bitcoin becomes divided into smaller and smaller units (on average). This is the result of increasing demand combined with a fixed supply, and the value of the network actually increases as a function of this process. As a network, bitcoin becomes more valuable as it is valued by more people. Essentially, 0.1 bitcoin = \$1,000 is more valuable than 1.0 bitcoin = \$1,000, despite each being worth the same measured in dollar terms. More exchange becomes possible as bitcoin becomes more valuable, with value being the output of more and more people choosing to adopt

bitcoin as an exchange intermediary. Each individual owns a smaller and smaller nominal amount of currency, but each equivalent unit's purchasing power increases over time. With each exchange, every individual is conveying their own value onto the network and is doing so at the direct expense of a competing monetary network. This process determines a new price specific to the value created and measured by each individual. As a result, bitcoin accumulates more information derived from a more diverse set of trading partners.

While prices today may not yet be quoted in bitcoin terms, a pricing system is forming every time an individual converts value into bitcoin. Even if dollars are an indirect intermediary, value produced somewhere in the world, distinct to a particular individual, is expressed as a unit of bitcoin. As more and more people choose to do so and increasingly on a per-individual basis, that value converts to a smaller and smaller unit of bitcoin (on average). The consequence is that more people can use a smaller and smaller denomination of bitcoin to transfer an equivalent amount of value, and as bitcoin is measured by more people—and more goods are priced or valued in bitcoin terms—its ability to measure relative value only increases. Since bitcoin can measure all value and can support adoption by a limitless number of individuals, it practically obsoletes the need for any other value-transfer network over the long term. Finite scarcity combined with divisibility creates an extremely powerful exchange intermediary. Bitcoin has the lowest terminal rate of change possible due to its absolute scarcity, and it can be divided into a fraction of a penny—which combined, will allow it to measure value far more precisely than any other currency.

The Greatest Exchange Tool—Transferability

With this baseline, the real knockout punch is the fact that bitcoin can be transferred, on an irrevocable basis, over a communication channel without needing a trusted third party as an intermediary. This is fundamentally different from digital payments in fiat systems, which depend entirely on trusted intermediaries. In aggregate, bitcoin is a greater constant than any

other form of money, is highly divisible and measurable, and is capable of being transferred over the internet with reliable final settlement. Try to identify a single other good that could possibly share these properties: finite scarcity (greatest constant) + divisibility and fungibility (measurement) + the ability to send over a communication channel (ease of transfer). This is what every other monetary good is up against as it competes for the convergent role of money. The only way to truly appreciate the power of such a rare dynamic is by experiencing it firsthand. Any individual can access the network on a permissionless basis by running a bitcoin node on a home computer. The ability to power up a computer anywhere in the world and transfer a finitely scarce resource to any other individual without permission or reliance on a trusted third party is empowering. That hundreds of millions of people can do this in unison without anyone needing to trust other participants in the network is near-impossible to fully comprehend.

Bitcoin is often described as digital gold, but this does not do it justice. Bitcoin combines the strengths of physical gold and the strengths of the digital dollar without the limitations of either. Gold is scarce but difficult to divide and transfer. The dollar is easy to transfer but lacks scarcity. Bitcoin is finitely scarce, easy to divide, and easy to transfer. In their current forms, gold as well as all fiat monetary systems depend on trust, whereas bitcoin is trustless. Bitcoin has optimized for the strengths and weaknesses of both, which is fundamentally why the market is converging (and will continue to converge) on bitcoin to fulfill the function of money.

Bitcoin Obsoletes All Other Money

If any individual comes to the following three conclusions, that individual is going to more consciously seek out the best form of money.

1. Money is a basic necessity.
2. Money is not a collective hallucination.
3. Economic systems converge on a single form of money.

Money is the economic good that preserves value into the future and allows individuals to convert their own time and skills into a range of choice so great that prior generations would find it difficult to imagine. Freedom is ultimately what a reliable form of money provides: freedom to pursue individual interests (specialization) and convert the output of that value into the value created by others (trade). Whether individuals consciously ask themselves these questions or not, they will be forced to answer them through their actions. Even those who do not will also arrive at the same answer as those who do. The conscious and the subconscious arrive at the same place because the fundamental truths do not change, and the function of money is singular: to intermediate a series of present and future exchanges by providing the baseline to communicate subjective value among a broad group of individuals who stand to benefit from trade and specialization. Money is a basic necessity. It is not a collective hallucination. And there are discernible properties that make certain goods more or less functional in exchange, which is an inherently intersubjective problem.

Owning bitcoin is becoming the cost of entry to what will likely be the largest and most diverse economy ever to exist. Bitcoin is global, and it is accessible on a permissionless basis. Because bitcoin becomes the common language of value for all participants, anyone that is a part of the network will be able to communicate and ultimately trade with other network participants. The more trading partners there are in the network, the greater the value each unit provides to currency holders. While there will likely always be jurisdictional friction that impedes trade, access to the same common currency removes the root source of friction in the communication and exchange of value, and bitcoin's fixed supply will allow its pricing mechanism to accumulate and communicate information with the least distortion relative to any other form of money. And as more individuals choose to store value in bitcoin, its fixed supply becomes more credible and its pricing mechanism more reliable and relevant. New adopters of a monetary network contribute value and realize value as a function of adoption, which is why it is not possible to be late to bitcoin, nor will bitcoin ever be too expensive.

At the end of the day, it does not matter how complicated bitcoin may seem. The decision to adopt bitcoin becomes an A/B test. The need for money is real, and individuals will converge on the form of money that best fulfills the function of exchange. No other currency in the world can ever be more scarce than bitcoin, and scarcity will act as a gravitational force, driving adoption and the communication of value. Today, most billionaires do not understand bitcoin. Bitcoin is an equal opportunity mind-bender. But even those who do not understand bitcoin will come to rely upon it. There are many fundamental questions. Bitcoin is volatile, seemingly slow, faces challenges to scaling, is not commonly used for payments, consumes a lot of energy, etc. Stability is an emergent property that will follow from broader adoption, and all other perceived limitations will be solved as a function of the value that is derived from finite scarcity combined with the ability to measure, divide, and transfer value. That is the innovation of bitcoin. Currency A has a fixed supply, while Currency B does not. Currency A continues to increase in value relative to Currency B. Currency A also continues to increase in purchasing power relative to goods and services, while Currency B does the opposite. Which one do I want? A or B? Choose wisely because the opportunity cost is your time and value. In practice, it all comes down to common sense and survival instincts. Bitcoin obsoletes all other money because economic systems converge on a single currency, and bitcoin has the most credible monetary properties.

CHAPTER TWO

Bitcoin, Not Blockchain

(Originally published on 6 September 2019)

Parsing the Landscape

Have you ever heard a smart-sounding person say that they are not sure about bitcoin but believe in blockchain technology? The stance is common and has given rise to the popular but misinformed narrative that “Blockchain, Not Bitcoin” is the real innovation. The idea that ‘blockchain’ technology is valuable but not bitcoin is the equivalent of saying you believe in airplanes but are unsure about the wings. And anyone who holds this view unknowingly communicates that he or she does not understand either.

Bitcoin and its blockchain are dependent on each other. However, for those new to bitcoin, understanding how it works and parsing the landscape can be overwhelming. Given the complexity and sheer volume of noise, who has the time to evaluate everything thoroughly? A more manageable path exists, but you have to know where to start. While there are seemingly thousands of cryptocurrencies and blockchain initiatives, there is really only one that matters: bitcoin. If you want to understand bitcoin or anything tangentially related, ignore everything as if it did not exist and try first to understand why bitcoin exists and how it works. That is the best foundation from which to then consider the entirety of everything else.

Setting biases aside, bitcoin is also the most practical entry point. There is no promise that you will come to the same conclusion that bitcoin is the

fundamentally valuable innovation, but more often than not, those who take the time to intuitively understand how and why bitcoin works are more easily able to recognize the flaws inherent in other blockchain projects. And even if not, starting with bitcoin remains your best hope of making an informed and independent assessment. Ultimately, bitcoin is not about making money and it's not a get-rich-quick scheme. It is fundamentally about storing the value you have already created, and no one should risk that without a requisite knowledge base. Within the world of digital currencies, bitcoin has the longest track record to assess and the greatest number of resources to educate, which is why bitcoin is the best tool to learn.



FIGURE 2.1

Michael Caras, *Bitcoin Money* (2019); Saifedean Ammous, *The Bitcoin Standard* (2018); Yan Pritzker, *Inventing Bitcoin* (2019); Andreas Antonopoulos, *Mastering Bitcoin* (2017); Jimmy Song, *Programming Bitcoin* (2019).

To start on this journey, first realize that bitcoin was created to specifically address a problem with modern money. The inventor of bitcoin set out to create a peer-to-peer digital cash system without the need for a trusted third party, and a blockchain was one critical part of the solution. In practice, bitcoin (the currency) and its blockchain are interdependent. One does not exist without the other. Bitcoin needs its blockchain to function, and there would not be a functioning blockchain without a native currency (bitcoin) to incentivize resources to protect it adequately. That native currency must be viable as a form of money because it is exclusively what pays for security, and it must have credible monetary properties in order to be viable.

Without the money, there is no security. And without the security, the value of the currency and the integrity of the data recorded by a blockchain

both break down. For this reason, a blockchain is only useful within the application of money, and money does not magically grow on trees. It really is that simple. A blockchain is only good for one thing, removing the need for a trusted third party, which only works in the context of money. A blockchain cannot enforce anything that exists outside the network. While a blockchain would *seem* to be able to track ownership outside the network, it can only *enforce* ownership of the currency that is native to its network. Bitcoin *tracks* ownership and *enforces* ownership. If a blockchain cannot do both, any records it keeps will be inherently insecure and ultimately subject to change. In this sense, immutability is not an inherent trait of a blockchain but instead, an emergent property. And if a blockchain is not immutable, its currency will never be viable as a form of money because transfer and final settlement will never be reliably possible. Without reliable final settlement, a monetary system is not functional and will not be adopted nor attract liquidity through exchange.

Monetary systems converge on one medium because their utility is liquidity and exchange rather than consumption or production. The market for exchange, and ultimately liquidity, consolidates around the form of money that is the **most secure**, long-term store of value. It would be irrational to store wealth in a less secure, less liquid form of money if a more secure, more liquid network existed as an accessible option. The aggregate implication is that only one blockchain is viable and ultimately necessary. Every other cryptocurrency is competing for the identical use case as bitcoin, that of money. Some realize it, while others do not. Regardless, value continues to consolidate around bitcoin because it has the **most secure** blockchain by orders of magnitude—the one least susceptible to arbitrary or unexpected change. Understanding these concepts is fundamental to bitcoin and provides a foundation to then consider and evaluate the noise beyond bitcoin. With a rudimentary knowledge of how bitcoin works, it becomes clear why there is no blockchain without bitcoin.

There Is No Blockchain

Bitcoin's transaction ledger is often thought of as a public blockchain that lives somewhere in the cloud, like a digital public square where all transactions are aggregated. However, there is no central source of truth. There are no oracles, and there is no central public blockchain to which everyone independently commits transactions. Instead, every participant within the network constructs and maintains its own independent version of the blockchain based on a common set of rules. No one trusts anyone and everyone validates everything. Participants are able to come to the same version of the truth without having to trust any other party. This is core to how bitcoin solves the problem of removing third-party intermediaries from a digital cash system in the validation and final settlement of exchange.

Independent Verification of New Blocks by Full Nodes

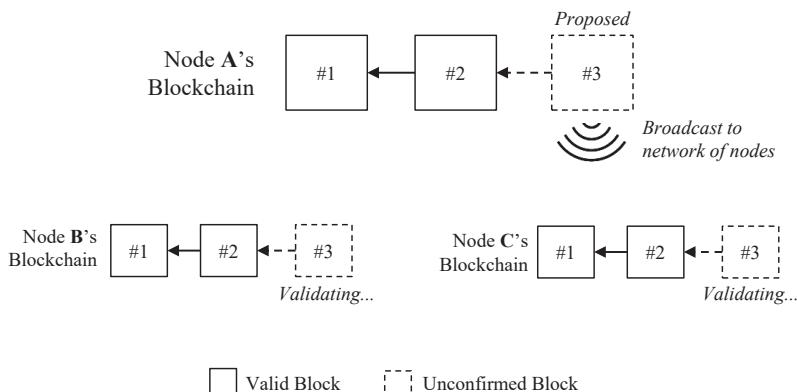


FIGURE 2.2

Every participant running a node within the bitcoin network verifies every transaction and every block independently. In doing so, each node aggregates its own independent version of the blockchain. Consensus is reached across the network because each node validates every transaction

(and block) based on a common set of rules whereby the longest valid chain is recognized. If a node broadcasts a transaction or block that does not follow consensus rules, other nodes will reject it as invalid. Through this function, the bitcoin network is able to converge on the same consistent state of ownership and dispose of the need for a central third party. However, the currency plays an integral role in coordinating bitcoin's consensus mechanism and ordering blocks, which ultimately represent bitcoin's complete and valid transaction history (or its blockchain).

Blocks and Mining

Think of a block as a dataset that links the past to the present. Technically, individual blocks record changes to the overall state of bitcoin ownership within a given time interval. In aggregate, blocks record the entire history of bitcoin transactions and, therefore, ownership of all bitcoin at any point in time. Only changes to the state of ownership are recorded in each passing block. How blocks are constructed, solved, and validated is critical to the process of network consensus, which also ensures that bitcoin maintains a fixed supply of 21 million. Miners compete to construct and solve blocks, proposing valid blocks to the rest of the network for acceptance. Think of the mining function as a continual process of validating history and clearing pending bitcoin transactions. Because bitcoin is permissionless, anyone can contribute resources to the mining function, but typically, bitcoin miners are run as specialized businesses. With each block, miners add new transaction history to the blockchain and validate the entire history of the chain. Miners secure the network through this function. However, all network nodes then subsequently check the work performed by miners for validity, ensuring network consensus is enforced. More technically, miners construct blocks that include three critical elements (simplified for clarity):

1. Reference to the prior block (validate the entire history of the chain)

2. Bitcoin transactions (clear pending transactions, i.e., changes to the state of ownership)
3. Coinbase transaction and transaction fees (compensation to miners for securing the network)

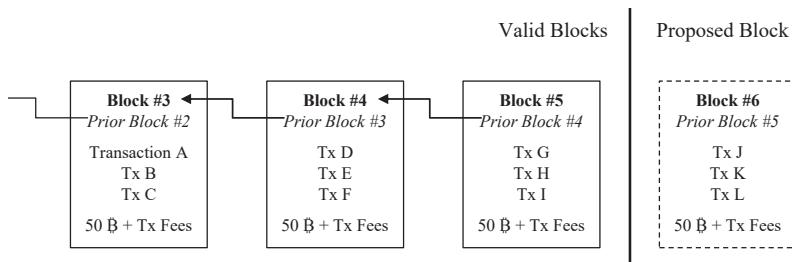


FIGURE 2.3

Miners solve blocks by expending energy resources to perform what is known as a proof-of-work function. For blocks to be valid, all inputs must be valid, and each block must satisfy the current network difficulty, which is directly tied to the then aggregate amount of energy resources securing the network. As more resources secure the bitcoin network, the network difficulty increases and the network becomes more secure, rather than the terminal supply of the currency increasing. To satisfy the network difficulty, a random value (referred to as a “nonce”) is added to each block, and then the combined dataset is run through bitcoin’s native cryptographic hashing algorithm (SHA-256). The resulting output (or hash) must achieve the network’s difficulty in order to be valid. Think of this as a simple “guess and check” function, but probabilistically, trillions of random values must be guessed and checked in order to create a valid proof for each proposed block. The addition of a random nonce may seem extraneous. But this function is what forces miners, by design, to expend significant energy resources in order to solve a block, which ultimately makes the network more secure by making it extremely costly to attack.

Adding a random nonce to a proposed block, which is an otherwise static dataset, causes each resulting output (or hash) to be unique. Imagine a dataset

being changed a trillion times, by just changing one single random number in the dataset each time. Everything else but the random nonce remains the same. With each nonce checked, the resulting output has an equally small chance of achieving the network difficulty (i.e., representing a valid proof). While this process is often referred to as solving a highly complicated mathematical problem, in reality, it is difficult only because a valid proof requires guessing and checking trillions of possible solutions. There are no shortcuts. Energy must be expended. A valid proof is easy to verify by other nodes but probabilistically impossible to solve without expending a massive amount of resources. As more mining resources are added to the network, the network difficulty increases, requiring more inputs to be checked and more energy resources to be expended to solve each block. Essentially, miners face a material cost in solving blocks, but it remains trivial for all other nodes to validate the work at practically no cost.

Proof-of-Work Function (Simplified)

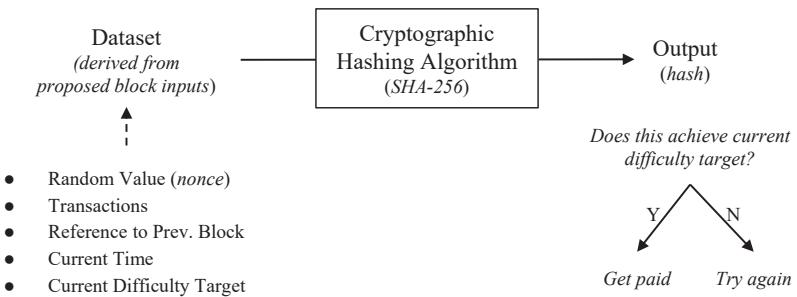


FIGURE 2.4

In aggregate, the incentive structure allows the network to reach consensus. Miners must incur significant up-front costs to secure the network but are only paid if valid work is produced. The rest of the network can immediately determine whether work is valid or not based on consensus rules. While there are many consensus rules that determine whether a block is valid or not, if any

pending transaction in a block is invalid, the entire block is invalid. For a transaction to be valid, it must have originated from a previously valid bitcoin block, and it cannot be a duplicate of a previously spent transaction. Separately, each block must build off of the most up-to-date version of history and include a valid coinbase transaction. A coinbase transaction rewards miners for producing valid work with newly issued bitcoin in return for securing the network (i.e., for enforcing the fixed supply and verifying valid transactions).

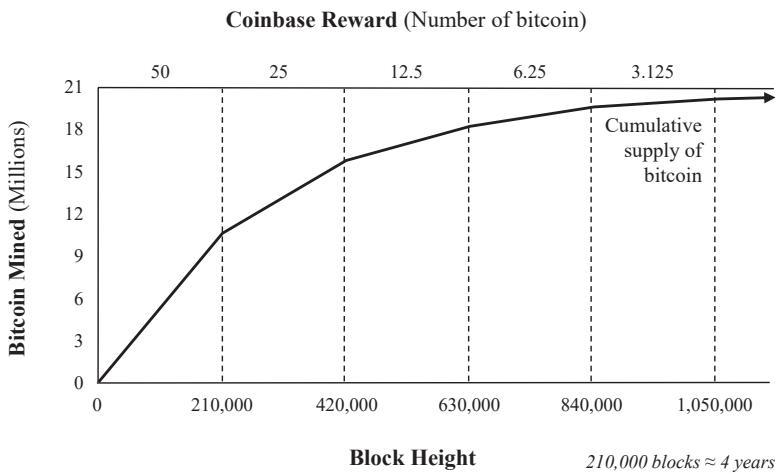


FIGURE 2.5

Coinbase rewards are governed by a predetermined supply schedule. At the time of writing, 12.5 new bitcoin are issued in each valid block, and the reward will be cut in half to 6.25 new bitcoin in approximately eight months. Every 210,000 blocks (or approximately every four years), the coinbase reward is reduced by half until it ultimately reaches zero. If miners include an invalid reward in a proposed block, the rest of the network will reject it as invalid. This is the base mechanism that governs bitcoin's capped total supply of 21 million. However, software alone is insufficient to ensure either a fixed supply or an accurate transaction ledger. Economic incentives hold everything together.

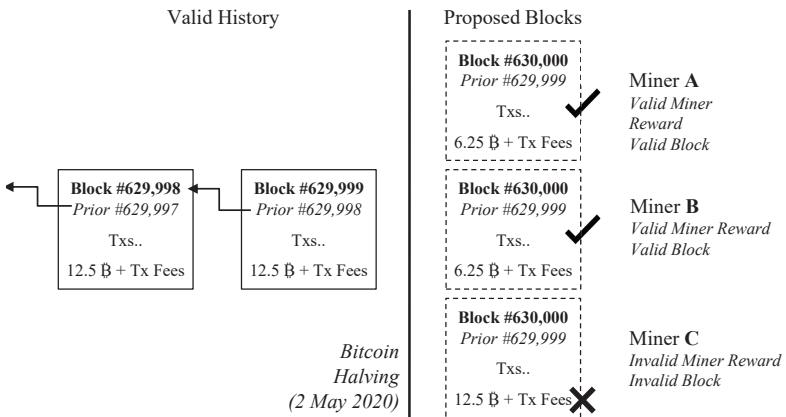


FIGURE 2.6

Consensus on a Decentralized Basis

Within one integrated function, miners validate history, clear transactions, and get paid for security on a trustless basis. The integrity of bitcoin's fixed supply is embedded in its security function. Because the rest of the network independently validates the work, consensus can be reached on a decentralized basis. If a miner completes valid work, the miner can rely on the fact that it will be paid on a trustless basis. Conversely, if a miner completes invalid work, the rest of the network enforces the rules, essentially withholding payment until valid work is completed. And the supply of the currency is baked into validity. If a miner wants to be paid, the miner must also enforce the fixed supply of the currency, further aligning the entire network. The incentive structure of the currency is so strong that everyone is forced to adhere to the rules, which is the chief facilitator of decentralized consensus.

If a miner solves and proposes an invalid block, specifically one that either includes invalid transactions or an invalid coinbase reward, the rest of the network will reject it as invalid. Separately, if a miner builds off of a version of history that does not represent the longest chain with the greatest proof-of-work, any proposed block would also be considered invalid.

Essentially, as soon as a miner sees a new valid block proposed in the network, it must immediately begin to work on top of that block (with a block height plus one) or risk falling behind and performing invalid work at a sunk cost. Consequently, in either scenario, if a miner were to produce invalid work, the miner would incur real costs but receive no compensation in return.

Through this mechanism, miners are financially incentivized at all times to work within the consensus of the chain to produce valid work. It is also why the higher the cost to perform the work, the more secure the network becomes. The more energy required to write or rewrite bitcoin's transaction history, the lower the probability that any single miner could (or would) be able to undermine the network. The incentive to cooperate increases as it becomes more costly to produce work that would otherwise be considered invalid by the rest of the network. As network security increases, bitcoin becomes more valuable. As the value of bitcoin rises and as the cost to solve blocks increases, the incentive to produce valid work increases (more revenue but more cost), while the penalty for invalid work becomes more punitive (no revenue and more cost).

Why don't some miners collude to undermine the network? First, they can't. Second, they tried.⁴ And third—the fundamental reason—as the network grows, it becomes more fragmented, and the economic value compensated to miners in aggregate increases. From a game-theory perspective, more competition and greater opportunity cost make it harder to collude. All the while, network nodes validate the work performed by miners, which acts as a constant check and balance. Miners are merely paid to perform a service, and the more miners there are, the greater the incentive to act in the interests of the network because the probability that a miner is penalized for invalid work increases as more competition exists. And recall that random nonce value. It seemed extraneous at the time, but it is core to the function that requires energy resources be expended. This tangible cost gives miners

4. Phil Geiger, "Bitcoin Refuses to Centralize," *Keeping Stock* (blog), Medium, 27 August 2018.

skin in the game. And when combined with the value of the currency, it is what incentivizes valid work and allows the network to reach consensus.

Because miners are maximally penalized for invalid work and all network nodes independently validate blocks, the network is able to form a consensus as to the accurate state of the chain without relying on any single source of knowledge or truth. None of this decentralized coordination would be possible without bitcoin, the currency. The bitcoin network *only* has its native currency to compensate miners in return for security, whether that is largely in the form of newly issued bitcoin today or exclusively in the form of transaction fees in the future. If the compensation paid to miners were not reasonably considered to be a reliable form of money, the incentive to make the investments to perform the work would not exist.

The Role of Money in a Blockchain

Recall from “Bitcoin Obsoletes All Other Money” that if an asset’s primary (if not sole) utility is in its exchange for other goods and services, and if it does not have a claim on the income stream of a productive asset (e.g., a stock or bond), it must compete as a form of money and will only store value if it possesses credible monetary properties. Bitcoin is a bearer asset, and it has no utility other than the exchange for other goods or services. It also has no claim on the income stream of a productive asset. Bitcoin is only valuable as a form of money and holds value because it has credible monetary properties. The only thing *any* blockchain can offer in return for security is a monetary asset native to the network, and one without any *enforceable* claims outside the network. This is why a blockchain can only be useful in connection to the application of money.

Without a native currency, a blockchain must rely on trust—i.e., the intervention of one or more third parties—for security, which eliminates the need for a blockchain in the first place. The security function of bitcoin (i.e., mining), which protects the validity of the chain on a trustless basis, requires significant up-front capital investment and ongoing marginal

costs in the form of energy consumption. To recoup that investment and provide a rate of return in the future, the payment in the form of bitcoin must more than offset the aggregate costs. If it were not expected to do so, such investments would not be made. Essentially, what miners are paid to protect (bitcoin) must be a reliable form of money to incentivize security investments.

Blockchain Decision Tree

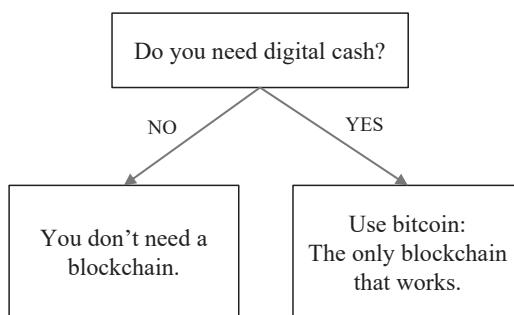


FIGURE 2.7

Source: *The Bitcoin Standard* by Saifedean Ammous

This is also fundamental to the incentive structure that aligns the network. Miners have an embedded incentive not to undermine the network because it would directly undermine the value of the currency in which miners are exclusively compensated. If bitcoin were not valued as money, there would be no miners, and without miners, there would be no chain worth protecting. The validity of the chain is what miners are paid to protect. If the network could not adequately come to a consensus and ownership were subject to change, no one could reasonably rely on bitcoin as a value-transfer mechanism. The value of the currency ultimately protects the chain, and the chain's immutability is foundational to the currency having value. It's an inherently self-reinforcing relationship.

Immutability Is an Emergent Property

As mentioned earlier, immutability is an emergent property in bitcoin, not an inherent trait of a blockchain. A global, decentralized monetary network with no central authority could not function without an immutable ledger (i.e., if the history of the blockchain were insecure and subject to change). If settlement of the unit of value (bitcoin) could not reliably be considered final, no one would be willing to trade real-world value in return. As an example, consider the sale of a car in exchange for bitcoin. Assume the buyer takes physical possession of the car, and the car's title is successfully transferred. If bitcoin's record of ownership could easily be rewritten or altered (i.e., if the history of the blockchain could be changed), the buyer could wind up in possession of both the car and the bitcoin, while the seller could end up with neither. This is why immutability and final settlement are critical to bitcoin's function.

Recall that bitcoin has no knowledge of the outside world. It only "knows" how to issue and validate currency. Bitcoin is an entirely self-contained system and is not capable of enforcing anything that exists outside the network (nor is any blockchain). For this reason, the bitcoin network can only ever validate one side of a two-sided value transfer. If bitcoin transfers could not reliably be considered final, it would be functionally impossible to trade anything of value in return for bitcoin. Hence, the immutability of bitcoin's blockchain is inextricably linked to the value of bitcoin as a currency. Final settlement in bitcoin is only possible because its ledger is reliably immutable. And its ledger is only reliably immutable because its currency is valuable. The more valuable bitcoin becomes, the more security it can afford. The greater the security, the more reliable and trusted the ledger.

Immutability is an emergent property dependent on other emergent network properties. As bitcoin becomes more decentralized, it becomes increasingly difficult to alter the network's consensus rules or to invalidate or prevent otherwise valid transactions (i.e., censorship resistance). As bitcoin

proves to be increasingly censorship-resistant, confidence in the network grows, fueling adoption, which further decentralizes the network, including its mining function. In essence, bitcoin becomes more decentralized and more censorship-resistant as it grows, which reinforces the immutability of its blockchain. It becomes increasingly difficult to change the history of the blockchain because each participant gradually represents a smaller and smaller share of the network. Regardless of how concentrated ownership of the network and mining may be at any point in time, both decentralize over time so long as value increases, which causes bitcoin to become more and more immutable.

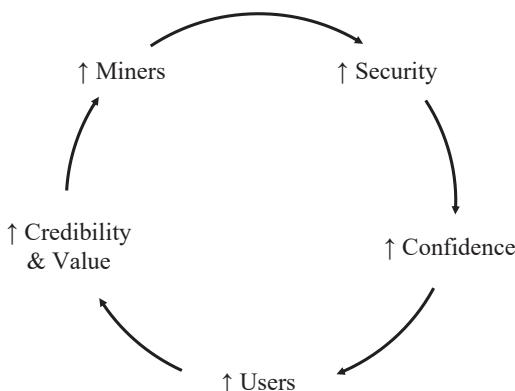


FIGURE 2.8

Bitcoin, Not Blockchain

Bitcoin's multidimensional incentive structure may be complicated, but it is critical to understand how bitcoin works and why bitcoin and its blockchain are interdependent. Each is a tool that relies on the other. Without one, the other is effectively meaningless. It is a symbiotic relationship that only works in the application of money.

Bitcoin as an economic good is only valuable as a form of money because it has no other utility. This is true of any asset native to a blockchain. The only

value bitcoin can ultimately provide is through present or future exchange. And the network is only capable of a single aggregate function: validating whether a bitcoin is a bitcoin and recording ownership over time.

The bitcoin network is an entirely independent, closed-loop system. Its only connection to the physical world is through its security and clearing function (mining and proof-of-work). The blockchain maintains a record of ownership, and the currency is used to pay for the security of those records. Through the value of its currency, the network can afford a level of security to ensure the immutability of the blockchain. As a result, network participants can consistently reach consensus without the need for trust in any third parties. The cumulative effect is a decentralized and trustless monetary system with a fixed supply that is global in reach and accessible on a permissionless basis.

Every fiat currency, commodity money (e.g., gold), and cryptocurrency is competing for the exact same use case as bitcoin, whether it is consciously understood by market participants or not. Bitcoin is valuable because, in aggregate, it has achieved finite scarcity. Scarcity is the backbone of why bitcoin is secure as a monetary network, and it is a property that is dependent on many other emergent properties.

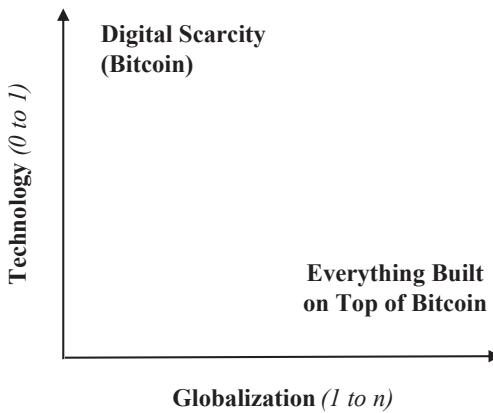


FIGURE 2.9

Inspired by *Zero to One* by Peter Thiel (2014)

A blockchain, on the other hand, is simply an invention native to bitcoin that enables the elimination of trusted third parties in a closed-loop monetary system. It serves no other purpose. It is only valuable in bitcoin as one piece to a larger puzzle and would be useless if it did not function in concert with the currency. The integrity of bitcoin's scarcity and the immutability of its blockchain are ultimately dependent on the value of the currency itself. Confidence in the aggregate function drives incremental adoption and liquidity, which reinforces and strengthens the value of the bitcoin network as a whole. As individuals opt in to bitcoin, they are simultaneously opting out of inferior monetary networks. This is fundamentally why the emergent properties in bitcoin are next to impossible to replicate and why its monetary properties become stronger over time (and with greater scale), all at the direct expense of inferior monetary networks.

Ultimately, a blockchain is only useful in the application of money because it is dependent on a native currency for security. All other blockchains are competing for the same fundamental use case. Bitcoin represents the most secure blockchain by orders of magnitude, and no other digital currency can compete because bitcoin's network effects only continue to increase its security and liquidity advantage over the field. Liquidity begets liquidity, and monetary systems converge to one medium as a derivative function.

The real competition for bitcoin has been, and will remain, the legacy monetary networks—principally the dollar, euro, yen, and gold. Think about bitcoin relative to these legacy monetary assets. Bitcoin does not exist in a vacuum; it represents a choice relative to other forms of money. Evaluate it based on the relative strengths of its monetary properties, and once a baseline is established between bitcoin and the legacy systems, this will then provide a strong foundation to more easily evaluate any other blockchain-related project.

CHAPTER THREE

Bitcoin Is Not Backed by Nothing

(Originally published on 27 September 2019)

Popular Misbelief

The critics often clamor like a broken record that “bitcoin isn’t backed by anything.” However, contrary to popular belief, bitcoin *is* backed by something. In fact, it is backed by the only thing that has ever backed any form of money: the credibility of its monetary properties. Money is not a collective hallucination, nor is it merely a belief system—two common myths. Over the course of history, various goods have emerged as money, and each time, it has not been by coincidence. Instead, these goods possessed properties that made them particularly useful and differentiated as a means of exchange—typically a combination of scarcity, durability, divisibility, fungibility, and portability, among others. With each emergent form of money, inherent properties of one medium improve upon and obsolete the monetary properties of a pre-existing form of money. Every time that one good has emerged as money, another was consequently demonetized. Essentially, the relative strengths of one monetary medium outcompete that of another. Bitcoin is no different. It represents a technological advancement in the global competition for money. Bitcoin is the superior successor to gold and the fiat money systems that leveraged gold’s monetary properties.

Bitcoin is finitely scarce, and it is easier to transfer than its incumbent competitors. It is also decentralized, and more resistant to censorship or

corruption as a result. There will only ever be 21 million bitcoin, and each bitcoin is divisible to eight decimal points (1 one-hundred millionth). Value can be transferred to anyone and to anywhere in the world on a permissionless basis without reliance on any third-party for final settlement. In aggregate, bitcoin is outcompeting its analog predecessors based on the credibility of its monetary properties, which are vastly superior to any other form of money used today. However, the key word is *credibility*. The emergent monetary properties in bitcoin are secured and reinforced through a combination of cryptography, a network of decentralized nodes enforcing a common set of consensus rules, and a robust mining network ensuring the integrity and immutability of bitcoin's transaction ledger. The currency itself is the keystone that binds the system together, creating economic incentives that allow the security columns to function as a whole. But even still, bitcoin's monetary properties are neither absolute nor considered in a vacuum. Instead, the strength and credibility of these properties are evaluated by the market *relative* to the properties inherent in other monetary systems.

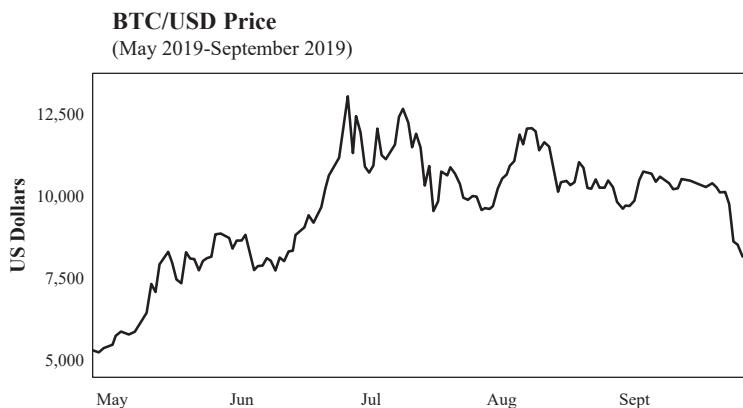


FIGURE 3.1

Source: Bitstamp

Recognize that every time a dollar is sold for bitcoin, the exact same number of dollars and bitcoin exist in the world. Exchanges between bitcoin

and dollars have no impact, at all, on the supply of either currency. Nothing changes except the market's preference to hold one currency versus the other. As the value of bitcoin rises, it is an indication that market participants increasingly prefer holding bitcoin over dollars. A higher price of bitcoin (in dollar terms) means more dollars must be sold to acquire an equivalent amount of bitcoin. In aggregate, it is an evaluation by the market of the relative strength of monetary properties. Price is the output. Monetary properties are the input. As individuals evaluate the monetary properties of bitcoin, the natural question becomes: which currency possesses more credible monetary properties? Bitcoin or the dollar? Well, what backs the dollar (or euro or yen, etc.) in the first place? When attempting to answer this question, the common refrain is that the dollar is backed by the government, the military (guys with guns), or taxes. However, the dollar is backed by none of these. Not the government, not the military, and not taxes. Governments tax what is valuable. A good is not valuable because it is taxed. Similarly, militaries secure what is valuable, not the other way around. Ultimately, a government cannot dictate the value of its currency. It can only control its supply and who has access.

Venezuela, Argentina, and Turkey all have governments, militaries, and the authority to tax, yet the currencies of each have deteriorated significantly over the past five years. While it's not sufficient to prove the counterfactual, each is an example that contradicts the idea that a currency derives its value as a function of government. Each and every occurrence of hyperinflation should be evidence enough of the inherent flaws in fiat monetary systems, but unfortunately it is not. Rather than acknowledging hyperinflation as the logical end game of all fiat systems, most simply believe hyperinflation to be evidence of monetary mismanagement. This simplistic view ignores first principles, as well as the dynamics that ensure monetary debasement in fiat systems. While the dollar is structurally more resilient as the global reserve currency, the underpinning of all fiat money is functionally the same, and the dollar is merely the strongest of a weak lot. As with all currencies, bitcoin is competing with the dollar based on the relative strengths of its monetary

properties. A baseline understanding of one is necessary to then compare and evaluate the other. After all, the competition is relative.

Why Does the Dollar Have Value?

The value of the dollar did not emerge on the free market. Instead, it emerged as a fractional representation of gold (and silver, initially). Essentially, the dollar was a solution to the limitations that existed in the convertibility and transferability of gold, having no inherent monetary properties of its own. From the onset, the dollar as a currency system was always based on trust: deposit gold at a bank, accept dollars in return, and trust that dollars could be converted back to gold at a fixed amount in the future. Gold's limitation and ultimate failure as money is the dollar system, and without gold, the dollar would have never existed in its current construct. Here is a quick review of the dollar's history with gold:

1900	The Gold Standard Act of 1900 established that gold was the only metal that could be converted into the dollar; gold was convertible to dollars at a rate of \$20.67 per oz.
1913	The Federal Reserve was created as part of the Federal Reserve Act of 1913.
1933	President Roosevelt banned the hoarding (saving) of gold via Executive Order 6102, requiring citizens to convert gold to dollars at \$20.67 per oz. or face a penalty in the form of a fine up to \$10,000 and/or up to five to ten years imprisonment.
1934	President Roosevelt signed the Gold Reserve Act, devaluing the dollar by approximately 40% to \$35 per oz. of gold.
1944	The Bretton Woods Agreement formalized the ability of foreign governments and central banks to convert gold to dollars (and vice versa) at \$35 per oz. and established fixed exchange ratios between dollars and other foreign currencies.
1971	President Nixon officially ended all convertibility of dollars to gold, effectively ending the Bretton Woods system. The value of the dollar was changed to \$38 per oz. of gold.

1973	The US government repriced gold to \$42 per oz.
1976	The US government then decoupled the value of the dollar from gold altogether in 1976.

Over the course of the twentieth century, the dollar transitioned from a reserve-backed currency to a debt-backed currency. While most people never stop to consider why the dollar has value in the post-gold era, the most common explanation remains that it is either a collective hallucination (i.e., the dollar has value simply because we all believe it does) or that it is a function of the government, the military, and taxes. Neither explanation has any basis in logic, nor is it the fundamental reason why the dollar retains value. Hundreds of millions of Americans are not all collectively hallucinating, and the dollar does not have value because of the military or the government's ability to tax. Instead, today, the dollar maintains its value as a function of debt and the relative scarcity of dollars to dollar-denominated debt. In the dollar world, everything is a function of the credit system. The mechanisms that fund the government (taxes and deficit spending) are both dependent on the credit system, and the credit system is what allows the dollar to function in its current construct.

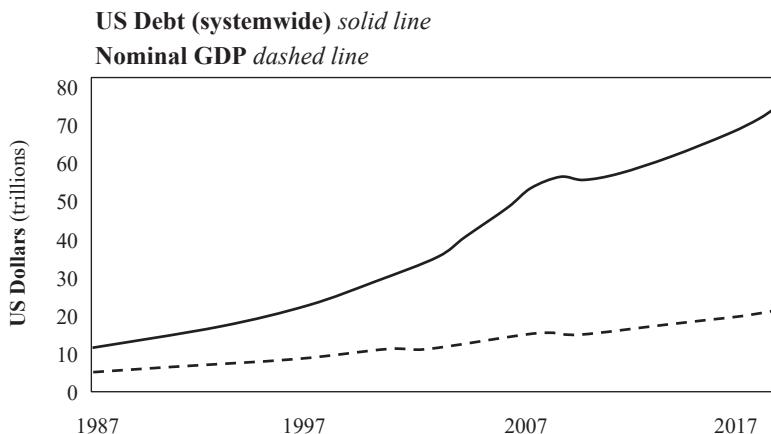


FIGURE 3.2
Source: Federal Reserve Economic Data (FRED)

The size of the credit system is several times larger than US nominal GDP, and it is orders of magnitude larger than the base money supply. Because of the credit system's relative size, economic activity in the US is largely coordinated through the allocation and expansion of credit. The chart below indexes the rate of change of the credit system compared to the rate of change of both nominal GDP and federal tax receipts (from 1987 to today). In the Fed's system, credit expansion drives nominal GDP, which ultimately dictates the nominal level of federal tax receipts.

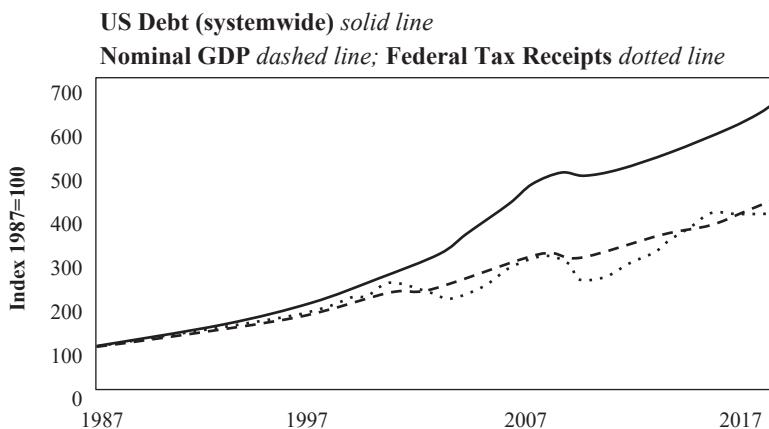


FIGURE 3.3
Source: Federal Reserve Economic Data (FRED)

As of the time of writing, there is \$73 trillion of dollar-denominated debt (fixed maturity / fixed liability) in the US credit system,⁵ but there are only \$1.6 trillion actual dollars in the banking system.⁶ Dollar debt creates future demand for dollars, and in the Fed's system, each dollar is leveraged approximately 40:1. If you borrow dollars today, you will need to source

5. Board of Governors of the Federal Reserve System (US), "All Sectors; Debt Securities and Loans; Liability, Level [TCMDO]," retrieved from Federal Reserve Economic Data (FRED), Federal Reserve Bank of St. Louis, 21 August 2019.

6. Board of Governors of the Federal Reserve System (US), *H.4.1: Factors Affecting Reserve Balances of Depository Institutions and Condition Statement of Federal Reserve Banks*, Federal Reserve Statistical Release, 26 September 2019.

dollars in the future to repay that debt, and currently, each dollar in the banking system is owed 40 times over. The relationship between the size of the credit system relative to the amount of dollars creates scarcity in the dollar. In aggregate, everyone needs dollars to repay dollar-denominated credit.

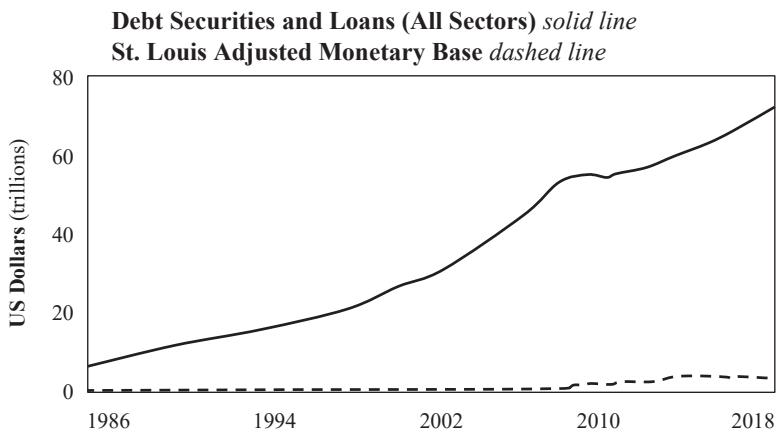


FIGURE 3.4
Source: Federal Reserve Economic Data (FRED)

The system as a whole owes far more dollars in debt than actually exist in circulation, creating an environment in which there is always a very high present demand for dollars. If consumers did not repay debt, homes would face foreclosure, and cars could be repossessed. If a corporation did not repay debt, company assets would be forfeited to creditors via a bankruptcy process, and equity could be entirely wiped out. If a government did not repay debt, basic government functions would be shut down due to lack of funding. In most cases, the consequence of not securing the future dollars necessary to repay debt means losing the shirt on your back. Debt creates the ultimate incentive to demand dollars. So long as dollars are scarce relative to the amount of outstanding debt, the dollar remains relatively stable and in very high demand. The Fed incentivizes credit creation by artificially reducing the cost of credit, which then creates the source of future demand for the underlying currency—like a drug dealer getting addicts hooked on

drugs, creating future dependency. In this case, the drug is debt, and it forces everyone, on average, to stay on the dollar hamster wheel.

The problem for the Fed's economy (and the dollar) is that it depends on the functioning of a highly leveraged credit system. And in order to sustain the amount of debt in the system, the Fed has to systematically increase the supply of actual dollars. Otherwise, the credit system would collapse. This is what quantitative easing is and why it exists (see *Bitcoin Fixes This*). Increasing the amount of base dollars has the immediate effect of deleveraging the credit system, but it has the longer-term effect of inducing more credit expansion. It also has the effect of devaluing the dollar gradually over time. This is all by design. Credit is ultimately what backs the dollar because what the credit actually represents is claims on real assets and, consequently, people's livelihoods. "Come with dollars in the future, or risk losing your house" is an incredible incentive to work for dollars.

The relationship between dollars and dollar credit keeps the Fed's game in play, and central bankers believe this can go on forever. Too much debt? Create more dollars. With more dollars, create more debt until there is too much, and so on. Ultimately, in the Fed's system (or any central bank's), the currency is the release valve. Because there is \$73 trillion of debt and only \$1.6 trillion actual dollars in the US banking system, more dollars will have to be added to the system to support the debt. The scarcity of dollars relative to the demand for dollars is what gives the dollar its value. Nothing more, nothing less. Nothing else backs the dollar. And while the dynamics of the credit system create relative scarcity of the dollar, it is also what ensures dollars will become less and less scarce on an absolute basis.

Too Much Debt → Create More Money → More Debt → Too Much Debt

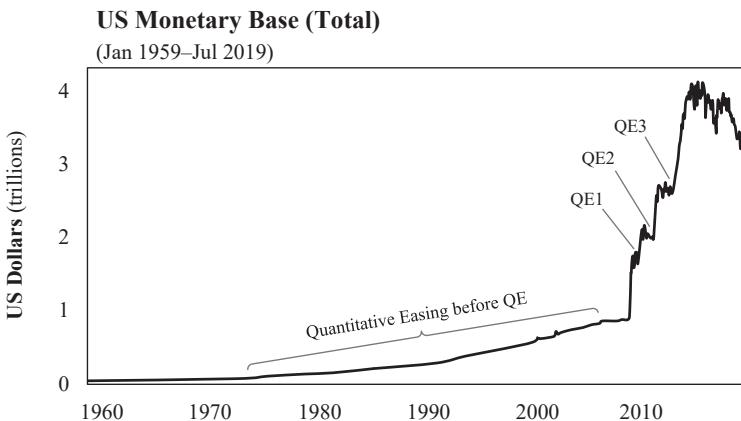


FIGURE 3.5
Source: Federal Reserve Economic Data (FRED)

As with any form of money, scarcity is the principal property that backs the dollar. But the dollar is only scarce relative to the amount of dollar-denominated debt that exists. And it now has real competition in the form of bitcoin. The dollar system and its lack of inherent monetary properties provides a stark contrast to the monetary properties emergent and inherent in bitcoin. The dollar system is based on trust. Bitcoin is not. The dollar's supply is governed by a central bank, whereas bitcoin's supply is governed by a consensus of market participants. The supply of dollars will always be wed to the size of its credit system, whereas the supply of bitcoin is entirely divorced from the function of credit. And the marginal cost to create dollars is zero, whereas the cost to create bitcoin is tangible and ever-increasing. Ultimately, bitcoin's monetary properties are emergent and increasingly unmanipulable, whereas the dollar is inherently and increasingly manipulable. And everything true of the dollar is true of any central bank's currency.

Money and Digital Scarcity

When evaluating bitcoin as money, the hardest mental hurdle to overcome is often its digital nature. Bitcoin is not tangible, and on the surface, it is not intuitive. How could something that is entirely digital be money? The dollar is mostly digital, yet it remains far more tangible than bitcoin in the minds of most. While the digital dollar emerged from its paper predecessor and physical dollars remain in circulation, bitcoin is natively digital. With the dollar, there is a physical bill that anchors your mental model in the tangible world. With bitcoin, there is not. Bitcoin possesses far more credible monetary properties than the dollar, but the dollar has always been money. While the dollar may be anchored in time and the physical world, the supply of dollars has no limits. Bitcoin, on the other hand, is finitely scarce.

Remember that the dollar does not have any inherent monetary properties. No unique properties ground the dollar as a stable form of money, other than its relative scarcity to the amount of dollar-denominated debt. Instead, the dollar leveraged the monetary properties of gold in its ascent to global reserve status. As a result, when evaluating bitcoin, the principles-based question to consider is whether bitcoin shares the quintessential properties that caused gold to emerge as money. Did gold emerge as money because it was physical or because it possessed transcendent properties beyond being physical? Of all the physical objects in the world, why gold? Gold emerged as money not because it was physical but instead because its aggregate set of properties was unique and particularly well suited for storing and exchanging value. Most importantly, gold is scarce, fungible, and highly durable. While gold possessed many properties that made it superior to any money that came before it, its fatal flaw was that it was difficult to transport and susceptible to centralization, which is ultimately why the dollar emerged as its transactional counterpart.

As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:

- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose

and one special, magical property:

- can be transported over a communications channel

—Satoshi Nakamoto, August 2010⁷

Bitcoin shares the monetary properties that caused gold to emerge as a monetary medium, but it also improves upon gold's flaws. While gold is relatively scarce, bitcoin is finitely scarce, and both are extremely durable. While gold is fungible, it is difficult to assay. Bitcoin is fungible and easy to assay. Gold is difficult to transfer and highly centralized. Bitcoin is easy to transfer and highly decentralized. Essentially, bitcoin possesses all the desirable traits of both physical gold and the digital dollar combined in one, but without the critical flaws of either. When evaluating monetary mediums, first principles are fundamental anchor points. Ignore the conclusion or end point, and start by asking yourself: if bitcoin were actually scarce and finite, ignoring that it is digital, could that be an effective measure of value and ultimately a store of value? Is scarcity a sufficiently powerful property to allow bitcoin to emerge as money, regardless of whether the form of that scarcity is digital?

As a tool, money is used to measure and exchange value. It is the good that coordinates all other economic activity, and scarcity is money's most important and foundational property. Scarcity relative to more abundant consumption goods and capital goods is what allows money to collectively store, measure, and exchange value. The absolute quantity of money is less

7. Satoshi Nakamoto, "Re: Bitcoin Does NOT Violate Mises' Regression Theorem," BitcoinTalk, Satoshi Nakamoto Institute, 27 August 2010.

important than its properties of being scarce, measurable, and capable of being transferred in exchange for goods and services. Despite being digital, bitcoin is designed to provide absolute scarcity, which is why it has the potential to be such an effective form of money (and measure of value). There will only ever be 21 million bitcoin. It provides a medium with finite scarcity that can be easily transferred. Dollars may seem easy to transfer, but the Fed created \$100 billion new dollars just last week, with the click of a button. That is approximately \$5,000 for every bitcoin that will ever exist, created in just a week (and by only one central bank). Since the Great Financial Crisis, the Federal Reserve, the Bank of Japan, and the European Central Bank have collectively created \$10 trillion worth of new money, the equivalent of approximately \$500,000 per bitcoin. Despite dollars, euro, yen, and bitcoin all being digital, bitcoin is the only medium that is tangibly scarce and the only one with inherent monetary properties.

However, it is insufficient to simply claim that bitcoin is finitely scarce. Nor should anyone accept this as fact. It is important to understand how and why that is the case. Credibility is the key. How does bitcoin *credibly* enforce its fixed supply? Why can't more than 21 million bitcoin be created? Why can't bitcoin be copied? While there are many pieces to the puzzle, three key architectural elements allow bitcoin to function with a reliably fixed supply when woven together with the economic incentives of the currency itself:

- Network consensus and full nodes: enforce a common set of governing rules
- Mining and proof-of-work: validate transaction history and anchor bitcoin security in the physical world
- Private keys: secure the unit of value and ensure ownership is independent from validation

What Secures Bitcoin—Network Consensus and Full Nodes

Twenty-one million is not just a number guaranteed by software. Instead, bitcoin's fixed 21 million supply is governed by a consensus mechanism, and all market participants have an economic incentive to enforce the rules of the bitcoin network. While a consensus of the bitcoin network could theoretically determine to increase the supply of bitcoin such that it exceeds 21 million, an overwhelming majority of bitcoin users would have to collectively agree to debase their own currency to do so. In practice, a global and decentralized network of rational economic actors, operating within a voluntary, opt-in currency system, would not collectively and overwhelmingly form a consensus to debase the currency that they have all independently and voluntarily determined to use as a store of wealth. This economic incentive underpins and reinforces bitcoin's technical architecture and network effect.

In bitcoin, a full node is a computer or server that maintains a full version of the bitcoin blockchain. Full nodes independently aggregate a version of the blockchain based on a common set of network consensus rules. While not everyone that holds bitcoin runs a full node, everyone is able to do so, and each node validates all bitcoin transactions and all blocks. By running a full node, anyone can access the bitcoin network and broadcast transactions (or blocks) on a permissionless basis. And nodes do not trust any other nodes. Instead, each node independently verifies the complete history of bitcoin transactions based on a common set of rules, allowing the network to converge on a consistent and accurate version of history on a trustless basis—that is consensus.

The bitcoin network removes trust in any centralized third party through this mechanism, which hardens the credibility of its fixed supply. All nodes maintain a history of all transactions, allowing each node to determine whether any future transaction is valid. In aggregate, bitcoin represents the most secure computing network in the world because anyone can access it, and no one trusts anyone. The network is decentralized, and there are no

single points of failure. Each node is also a redundancy to every other node, from a record-keeping and validation perspective. Every node represents a check and balance on the rest of the network, and without a central source of truth, the network is resistant to attack and corruption. Any node could fail or could become corrupted, and the rest of the network would remain unimpacted. The more nodes that exist, the more decentralized bitcoin becomes, which increases redundancy and makes the network harder and harder to corrupt or censor.

Contrasting Monetary Systems

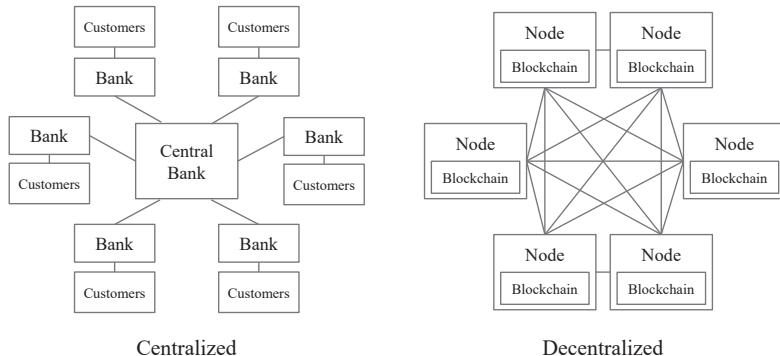


FIGURE 3.6

Each full node enforces the consensus rules of the network, a critical element of which is the currency's fixed supply. Each bitcoin block includes a predefined number of bitcoin to be issued, and each bitcoin transaction must have originated from a previously valid block in order to be valid. Every 210,000 blocks, the bitcoin issued in each valid block is cut in half until the amount of bitcoin issued ultimately reaches zero in approximately 2140, creating an asymptotic, capped supply schedule. Because each node independently validates every transaction and each block, the network collectively enforces the fixed 21 million supply. If any node were to broadcast an invalid transaction or block, the rest of the network would reject it and

that node would fall out of consensus. Essentially, any node could attempt to create excess bitcoin, but every other node has an interest in ensuring the supply of bitcoin is consistent with the predefined fixed limit. Otherwise, the currency would be arbitrarily debased at the direct expense of the rest of the network. No one has an incentive to allow others to arbitrarily create money, and everyone has the incentive to prevent it from happening.

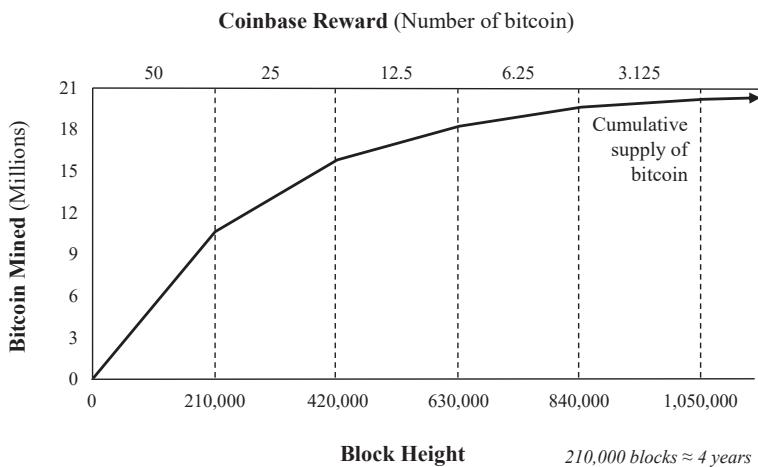


FIGURE 3.7

Separately, anyone within or outside the network could copy bitcoin's software to create a different version of bitcoin. But any currency units created by such a copy would be considered invalid by the nodes operating within the bitcoin network because the units would not have originated from a previously valid bitcoin block. Nor would anyone accept the currency as bitcoin. Each bitcoin node independently validates whether a bitcoin is a bitcoin. It would be like trying to pass off Monopoly money as dollars. No one would accept it as bitcoin, nor would it share the emergent properties or infrastructure of the bitcoin network. Running a bitcoin full node allows anyone to instantly assay whether a bitcoin is valid, and any copy of bitcoin would be immediately identified as counterfeit and invalid.

The consensus of nodes determines the valid state of the network within a closed-loop system. When anything occurs outside its walls—anything inconsistent with its consensus rules—it's as if it never happened.

What Secures Bitcoin—Mining and Proof-of-Work

As part of the consensus mechanism, certain nodes (referred to as miners) also perform bitcoin's proof-of-work function to add new bitcoin blocks to the blockchain. This function validates the complete history of transactions and clears pending transactions. The process of mining is ultimately what anchors bitcoin security in the physical world. To solve blocks, miners must perform trillions of cryptographic computations, which requires expending significant energy resources. Once a block is solved, it is proposed to the rest of the network for validation. All nodes (including other miners) verify whether a block is valid based on the common set of network consensus rules discussed previously. If any transaction in the block is invalid, the entire block is invalid. Separately, if a proposed block does not build on the latest valid block (i.e., the longest version of the block chain), the block is also invalid.

For context, at 90 exahashes per second, approximately 9 gigawatts of power distributed throughout the world currently secures the bitcoin network, which equates to ~\$11 million per day (~\$4 billion per year) of energy at a marginal cost of 5 cents per kWh (rough estimates). Blocks are solved on average every ten minutes, which translates to approximately 144 blocks per day. Across the network, each block currently requires approximately \$75,000 in energy expenditure to solve, and the reward per block is approximately \$100,000 (12.5 new bitcoin x \$8,000 per bitcoin as of the time of writing, excluding transaction fees). The higher the cost to solve a block, the more costly the network is to attack. The cost to solve a block represents the tangible resources it requires to write history to the bitcoin transaction ledger, which functionally clears transactions for final settlement. As the network grows, the network becomes more fragmented, and

the economic value compensated to miners in aggregate increases. From a game-theory perspective, more competition and greater opportunity cost make it harder to collude, and all network nodes validate the work performed by miners, which serves as a check and balance.

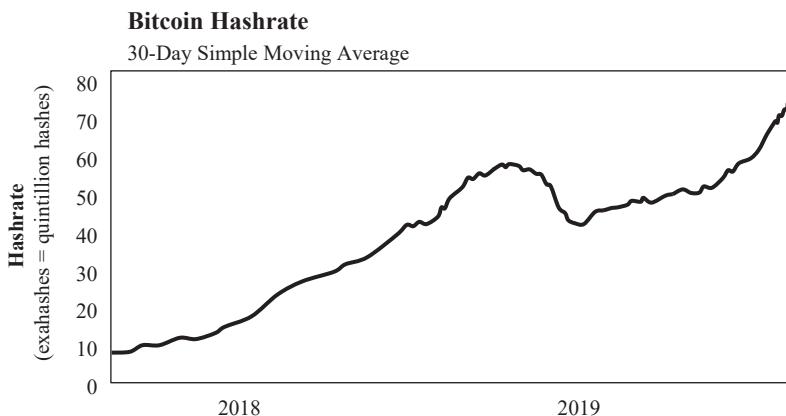


FIGURE 3.8
Source: bitinfocharts.com

Recall that a predefined number of bitcoin are issued in each valid block (that is, until the 21 million limit is reached). The bitcoin issued in each block combined with network transaction fees represent the compensation to miners for performing the proof-of-work function. Importantly, the miners are paid exclusively in bitcoin to secure the network. As part of the block construction and proposal process, miners include the predefined number of bitcoin—consistent with the fixed supply schedule—to be issued as compensation for expending tangible, real-world resources to secure the network. If a miner were to include an amount of bitcoin greater than the predefined supply schedule as compensation, the rest of the network would reject the block as invalid. As part of the security function, miners must validate and enforce the fixed supply of the currency in order to be compensated. Miners have material skin in the game in the form of up-front capital costs (and energy expenditure), and invalid work is not rewarded or compensated.

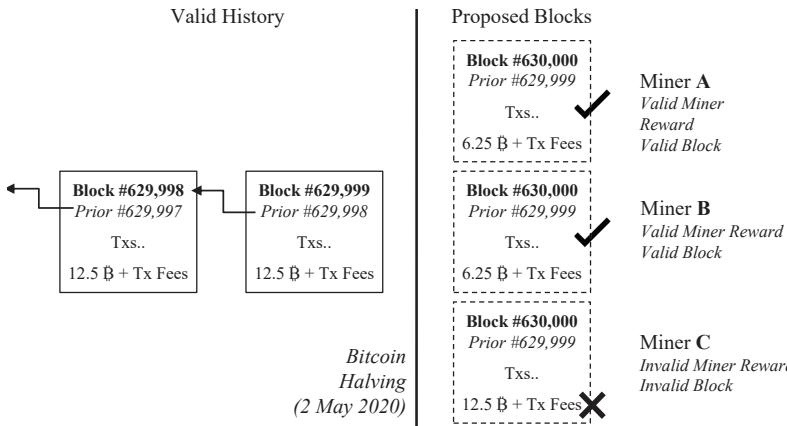
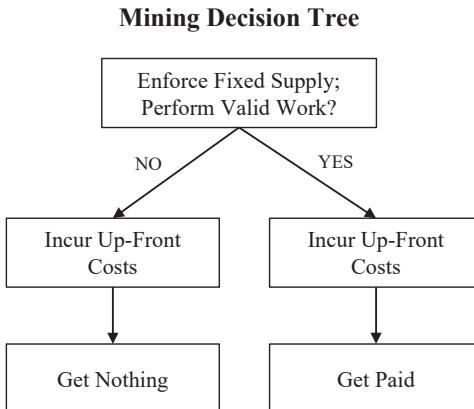


FIGURE 3.9

For a technical example, the valid reward paid to miners is halved every 210,000 blocks with the next halving of issuance scheduled to occur at block 630,000 (or approximately in May 2020). At that time and scheduled block, the valid reward will be reduced from 12.5 bitcoin to 6.25 bitcoin per block. Thereafter, if any miner includes an invalid reward (an amount greater than 6.25 bitcoin), the rest of the network will reject it as invalid. The halving event is important not just because the supply of newly issued bitcoin is reduced, but also because it demonstrates that the economic incentives of the network continue to effectively coordinate and enforce the fixed supply of the currency on an entirely decentralized basis. While bitcoin's fixed supply is actually enforced with each next block, the halving of the supply is a more tangible and observable datapoint to the outside world that the 21 million fixed supply is being enforced without any central coordination. If any miner ever attempts to cheat, it will be maximally penalized by the rest of the network. Nothing other than the economic incentives of the network coordinate this behavior. That it occurs on a decentralized basis without the coordination of any central authority reinforces the security of the network.

**FIGURE 3.10**

Because mining is decentralized and because all miners are constantly competing with all other miners, it is not practical for miners to collude. Separately, all nodes validate the work performed by miners, instantly and at practically no cost, which creates a very powerful check and balance that is divorced from the mining function itself. Miners are not the only constituents validating the work of other miners. Blocks are costly to solve but easy to validate by the entire network. In aggregate, this is a fundamental differentiator between bitcoin and the monetary systems with which bitcoin competes, whether gold or the dollar. And the compensation paid to miners for securing the network and enforcing the network's fixed supply is exclusively in the form of bitcoin, which further aligns incentives. Individual miners do not have an incentive to allow other miners to arbitrarily create more money, and there is an active disincentive to undermine the credibility of the currency that a miner is being paid to secure, especially given the sole compensation is in units of the very same currency. The economic incentives of the currency (compensation) are so strong and the penalty is both so severe and so easily enforced that miners are maximally incentivized to perform valid work. By introducing tangible cost to the mining process,

by incorporating the supply schedule in the validation process (which all nodes verify), and by divorcing the mining function from ownership of the network, the network as a whole reliably and constantly enforces the fixed supply (21 million) of the currency on a trustless basis.

What Secures Bitcoin—Private Keys and Equal Rights

While miners construct, solve, and propose blocks and while nodes check and validate work performed by miners, private keys control access to the unit of value itself. Private keys control the rights to the 21 million bitcoin (technically only 18.0 million have been mined to date). In bitcoin, there are no identities. Bitcoin knows nothing of the outside world. The bitcoin network validates signatures and keys. That's all. Only someone in control of a private key can create a valid bitcoin transaction by creating a valid signature. Valid transactions are included in blocks, which are solved by miners and validated by each node, but only those in possession of private keys can produce valid transactions.

When a valid transaction is broadcast, bitcoin is spent (or transferred) to specific bitcoin public addresses. Public addresses are derived from public keys, which are derived from private keys. Public keys and public addresses can be calculated using a private key, but a private key cannot be calculated from a public key or public address. It is a one-way function secured by advanced cryptography. Public keys and public addresses can be shared without revealing anything about the private keys. When a bitcoin is spent to a public address, it is essentially locked in a safe, and to unlock the safe to spend the bitcoin, a valid signature must be produced by the corresponding private key (every public key and address has a unique private key). The owner of the private key produces a unique signature, without revealing the secret itself. The rest of the network can verify that the holder of the private key produced a valid signature, without actually knowing any details of the private key itself. Public and private key pairs are the foundation of bitcoin. And ultimately, private keys control access rights to the economic value of the network—the units of currency.

Address Derivation for Private Key

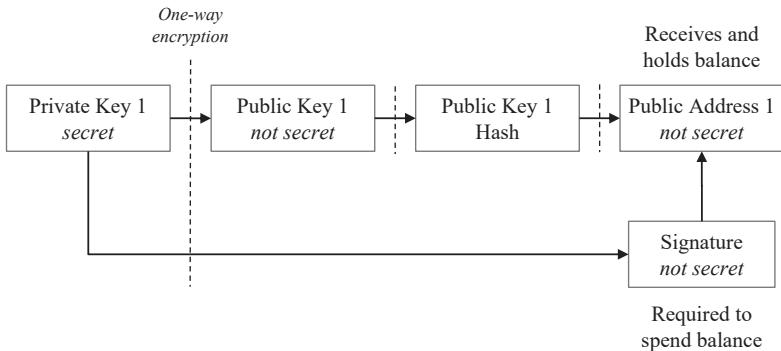


FIGURE 3.11

It doesn't matter whether someone has one-tenth of a bitcoin or ten thousand bitcoin. Either and each are secured and validated by the same mechanism and by the same rules. Everyone has equal rights. Regardless of the economic value, each bitcoin (and bitcoin address) is treated identically within the bitcoin network. If a valid signature is produced, the transaction is valid, and it will be added to the blockchain (if a transaction fee is paid). If an invalid signature is produced, the network will reject it as invalid. It does not matter how powerful or how weak any participant may be. Bitcoin is apolitical. All it validates are keys and signatures. Someone with more bitcoin may be able to pay a higher fee to have a transaction prioritized, but all transactions are validated based on the same set of consensus rules. Miners prioritize transactions based on value and profitability, nothing else. If a transaction is equally valuable, it will be prioritized based on a time sequence. But importantly, the mining function, which clears transactions, is divorced from ownership. Bitcoin is not a democracy. Ownership is controlled by keys, and every bitcoin transaction is evaluated based on the same criteria within the network. It is either valid or it is not. And every bitcoin must have originated within a block consistent with the 21 million supply schedule in order to be valid.

This is why users controlling keys is such an important and significant ethos in bitcoin. Bitcoin are finitely scarce, and private keys are the gatekeeper to the transfer of every bitcoin. The saying goes: not your keys, not your bitcoin. If a bank or other third party controls your keys, that entity is in control of your access to the bitcoin network, and it would be very easy to restrict access or seize funds in such a scenario. While many people choose to trust a bank-like entity, the security model of bitcoin is unique. Not only can each user control their own private keys, but each user who does can also access the network on a permissionless basis and transfer funds to anyone anywhere in the world. In aggregate, users controlling private keys decentralize the control of the network's economic value, which increases the security of the network as a whole. The more distributed network ownership and access is, the more challenging it becomes to corrupt or co-opt the network. Separately, by holding a private key, it becomes extremely difficult for anyone to restrict access or seize funds held by any individual. Every bitcoin in circulation is secured by a private key. Miners and nodes may enforce that only 21 million bitcoin will ever exist, but the valid bitcoin that do exist in circulation are ultimately controlled and secured by a private key.

Bitcoin Versus

In summary, the supply of bitcoin is governed by a network consensus mechanism, and miners perform a proof-of-work function that grounds bitcoin's security in the physical world. As part of the security function, miners get paid in bitcoin to solve blocks, which validate history and clear pending bitcoin transactions. If a miner attempts to compensate itself in an amount inconsistent with bitcoin's fixed supply, the rest of the network will reject the miner's work as invalid. The supply of the currency is integrated into bitcoin's security model, and real-world energy resources must be expended for miners to be compensated. Still yet, every node within the network validates the work performed by all miners, such that no one can cheat without a material risk of penalty. Bitcoin's consensus mechanism and validation process

ultimately governs the transfer of ownership of the network, but ownership of the network is controlled and protected by individual private keys held by users of the network.

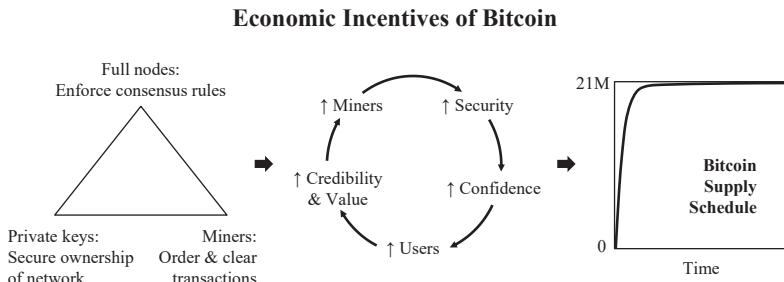


FIGURE 3.12

Set aside any preconceived notions of what money is, and imagine a currency system that has a credibly enforced fixed supply. A form of money that cannot be printed and is finite in supply. Anyone in the world can connect to the network on a permissionless basis and anyone can send transactions to anyone, anywhere in the world. Everyone can also independently and easily validate the supply of the currency as well as ownership across the network. Imagine a global economy where billions of people, disparately located throughout the world, can transact across one common decentralized network, and everyone can arrive at the same consensus of the ownership of the network, without the coordination of any central party. How valuable would that network be? Bitcoin is valuable because it is finite, and it is finite because it is valuable—because a currency with a fixed supply is worth securing. The economic incentives and governance model of the network reinforce each other. The cumulative effect is a decentralized and trustless monetary system with a fixed supply that is global in reach and accessible by anyone.

Bitcoin is distinct from all other digital forms of money, including the dollar, because it has inherent and emergent monetary properties. While the supply of bitcoin remains fixed and finitely scarce, central banks will be

forced to create more money in order to sustain the legacy credit system. Bitcoin will become more attractive as market participants figure out that future rounds of quantitative easing are not just a possibility but a necessity to sustain an inferior form of money. Before bitcoin, everyone was forced to opt in to this system by default. Now that bitcoin exists, there is a viable alternative. Each time the Fed returns with more quantitative easing to sustain the credit system, more and more individuals will discover that the monetary properties of bitcoin are vastly superior to the legacy system. Is A better than B? That is the test. In the global competition for money, bitcoin has inherent monetary properties that the fiat monetary system lacks. Ultimately, bitcoin is backed by something, and it's the only thing that backs any form of money: the credibility of its monetary properties.

CHAPTER FOUR

Bitcoin Is Antifragile

(Originally published on 12 June 2020)

Lacking a Baseline

If one thing is certain, it is that bitcoin is humbling. It humbles everyone—some sooner than others, but everyone eventually. Individuals you respect have likely called bitcoin a fraud or compared it to rat poison, but rest assured. If it hasn't been walked back yet, it will be in time. For most everyone first considering bitcoin, the proper context to evaluate it is practically nonexistent, which even applies to the most revered financiers of our time—like Warren Buffett. Is bitcoin like a stock, bond, tech startup, the internet, or merely a figment of everyone's imagination? At first glance, bitcoin admittedly makes very little sense. It is very reasonably believed by many to be one massive collective hallucination. There are two fundamental reasons: almost everyone lacks a baseline to evaluate bitcoin because there has never been anything like it, and very few people have ever consciously considered what money is.

Every day, people evaluate whether to invest in stocks, bonds, or real estate, whether to buy a home or car, whether to purchase some consumer good, or conversely, whether to save. While there are exceptions to every rule, practically everyone is unequipped to evaluate bitcoin because it does not fit any existing mental framework. It is like asking someone with no concept of mathematics what two plus two equals. The answer may be obvious

to those who know math, but for those who do not, it's wholly unrelatable. As an idea and application, bitcoin is incredibly abstract, largely because money is abstract. Trying to understand it can feel like staring into the abyss. Bitcoin is both difficult to see yet impossible to unsee once discovered. And the path from one extreme to the other is most often a journey, where the impossible first becomes possible, then probable, and ultimately inevitable for each individual.

Contrasting Monetary Systems

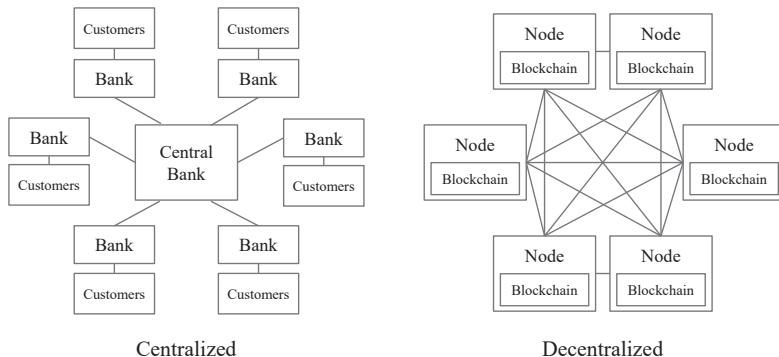


FIGURE 4.1

Eventually, some chord is struck, and dots are connected. As the fog begins to lift, there naturally remains the idea that while bitcoin is possible, it is surely subject to high degrees of chance and more likely to fail than succeed. It is perceived to be inherently fragile and risky. Many believe that bitcoin could vanish as quickly as it appeared on the scene. At the beginning of the journey, it seems to live somewhere between an aspiring long shot and just one unidentified silver bullet away from complete and utter collapse. Bitcoin is novel and often thought of as untested and unproven. Launched in 2009, it seemingly lacks permanence. It is not yet anchored in history. At the same time, bitcoin has been around for twelve years—as of the time of writing—and has a total purchasing power (or value) of \$180 billion. With more than

a decade of operating history and hundreds of billions in value, bitcoin may still be an upstart, but it is far from untested and unproven. In reality, bitcoin is thriving in the wild without any central coordination, and it is the lack of central coordination from which bitcoin gets its lifeblood. Decentralization not only allows bitcoin to function but also causes it to gain strength rather than falter when stressed.

Bitcoin is natively digital and powered by computers running software capable of being shut down, which lends to the default impression that bitcoin is inherently fragile. The mental image of a computer network being unplugged creates the false sense that bitcoin as a system could suddenly cease to exist, when the opposite is true for the very same reason. Bitcoin exists everywhere and nowhere. No one controls it, anyone can run bitcoin's open-source software from anywhere, hundreds of thousands of people do, and it's relied upon by a network of tens of millions (and growing). Decentralization gives bitcoin permanence. With no single point of failure, bitcoin is practically impossible to stop because it is impossible to control. It is a dynamic system that only becomes more redundant and further decentralized in time and with increasing adoption. In short, bitcoin is more permanent than risky because it is an antifragile system. Antifragile, an idea popularized by Nassim Taleb in his 2012 book of the same name, describes systems or phenomena that gain strength from disorder, which bitcoin is to its core. There is no silver bullet that can kill bitcoin. There is no competitor that can magically overtake it. There is no government or corporation that can shut it down. But it does not stop there. Each attack vector and shock to the system actually causes bitcoin to become stronger.

Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets

better. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes (say, chicken soup or steak tartare with a drop of cognac), the rise of cities, cultures, legal systems, equatorial forests, bacterial resistance ... even our own existence as a species on this planet. And antifragility determines the boundary between what is living and organic (or complex), say, the human body, and what is inert, say, a physical object like the stapler on your desk. [...] The antifragile loves randomness and uncertainty, which also means—crucially—a love of errors, a certain class of errors.

—Nassim Taleb⁸

A Positive Feedback Loop

Bitcoin is an adaptive and evolving system. It is not static. No one controls the network, and there are no leaders capable of forcing changes onto the network. It is decentralized at every layer, and as a result, it has shown itself to be immune to attack. However, it is not just immune. Bitcoin actually becomes stronger as:

1. external forces attempt to influence or co-opt the network;
2. individuals make errors within the network; or
3. as a function of its volatility—a trait often perceived as a limiting or critical flaw.

As bitcoin survives shocks and as individuals learn from their errors and adapt to its volatility, bitcoin becomes tangibly more reliable. The network's demonstration of resilience and immunity reinforces trust in the network, which drives incremental adoption and makes bitcoin more resistant to

8. Nassim N. Taleb, *Antifragile: Things That Gain from Disorder* (Random House, 2012), 3.

future attacks or individual errors. It is a positive feedback loop. With every failed attempt to co-opt or coerce the network, the bitcoin protocol hardens, and confidence increases. Every time bitcoin survives an attack, it is propelled forward in a fundamentally stronger state.

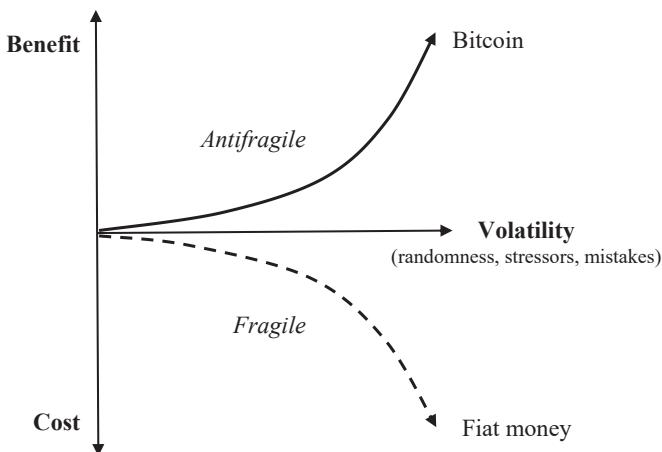


FIGURE 4.2

Each exogenous shock to the network provides learnings that cause bitcoin to adapt in spontaneous ways that can only be endemic to a decentralized system. Because bitcoin is decentralized and becomes increasingly decentralized with time (and adoption), not only is there no single point of failure, but the increasing levels of redundancy ensure network survival and fortify it against future attacks. There is a positive correlation between time and the degree of network decentralization. Similarly, there is a positive correlation between the degree of decentralization and the network's ability to fend off more formidable attacks. Essentially, as the network becomes more decentralized, it also becomes resistant to threats it may not have been capable of surviving in prior states.

As bitcoin grows, each potential point of failure becomes less critical to the proper functioning of the network as a whole. Errors made by individuals

are isolated to the responsible parties, weak points in the network are sacrificed, and the system strengthens in aggregate. The entire process is effective and efficient because it is never a conscious decision but simply structural to the system architecture. No one picks winners and losers. At all times, network participants are maximally accountable for their own errors. There are no bailouts. Decentralization simultaneously eliminates moral hazard and ensures system survival. Incentives and accountability optimize for innovation and naturally drive toward consistently better outcomes. While the incentive structure doesn't eliminate error, it ensures that errors are productive, allowing the network to adapt to threats and immunize around them. Whether borne from exogenous shocks or individual errors, bitcoin feeds on disorder, stressors, volatility, and randomness. Collectively, these are the hallmarks of an antifragile system.

Bitcoin Benefits from Disorder

The lack of social order in bitcoin may be its single greatest asset. There is no CEO of bitcoin, nor is there a centralized authority that controls it. There is no person or organization to drag in front of Congress, whether to answer questions or compel action. In fact, there is no Congress or legislative body with any influence over bitcoin, preferential or otherwise. It does not mean that any individual or company is immune from influence. Nor does it prevent any country from attempting to regulate (or ban) bitcoin, but disorder insulates the network from external threats. While Facebook's Libra is fundamentally plagued as a currency for reasons independent of government influence, the CEO and other top executives were quickly brought before Congress to answer questions soon after its announcement, with key legislators demanding the project be delayed, if not scrapped, over concerns of "national security" and other regulatory issues.⁹ It is not that

⁹ Hearing: *An Examination of Facebook and its Impact on the Financial Services and Housing Sectors*, Before the House Financial Services Committee, 116th Congress (23 October 2019) (questioning of Mark Zuckerberg, CEO and Chairman of Facebook).

CEOs and companies cannot coexist with government. Instead, it is that the mere existence—of governments, CEOs and companies—creates influence that could never exist in bitcoin at a protocol level, and the absence of which allows bitcoin to be viable as a currency.

“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

—Satoshi Nakamoto¹⁰

With no central counterparties controlling the network, bitcoin functions on a decentralized basis and in a state that eliminates the need for, or dependence on, trust. Its distributed architecture reduces the network’s attack surface by removing single points of failure that would otherwise expose the system to critical risk. Built on a foundation of social disorder, it is only in the absence of control that bitcoin is able to function on a secure basis. It is the polar opposite of the central bank trust-based model. Bitcoin is a monetary system built on a market consensus mechanism, rather than centralized control. There are certain consensus rules that govern the network. Each participant opts in voluntarily and everyone independently enforces the rules. If any market participant changes a rule to be inconsistent with the rest of the network, that participant falls out of consensus. The network consensus rules ultimately define what is and is not a bitcoin. Independent verification and the aggregate network enforcement function, on a decentralized basis, ensures there will be only 21 million bitcoin. By eliminating trust in centralized counterparties, all network participants can rely upon and ultimately trust that the monetary policy is secure and that it will not be subject to arbitrary change. This may seem paradoxical, but it is perfectly rational. The system is trusted *because* it is trustless, and it would not be trustless without high degrees of social disorder. Ultimately, spontaneous order

10. Satoshi Nakamoto, “Bitcoin Open Source Implementation of P2P Currency,” P2P Foundation, forum post, 11 February 2009.

emerges from disorder and strengthens as each exogenous system shock is absorbed.

In 2017, a civil war of sorts emerged in bitcoin. Many of the largest companies that provide bitcoin custody and exchange services aligned with many of the largest bitcoin miners (collectively controlling >85% of the network's mining capacity) in an attempt to force a change to the consensus rules. This group of power brokers wanted to double the bitcoin block size as a means to increase the network's transaction capacity. However, the proposal required a change to the network's consensus rules, which would have resulted in a split (or hard fork) of the network. As part of a negotiated "agreement," the group proposed to activate a significant network upgrade (referred to as SegWit, an upgrade that would not change the consensus rules). And at the same time, the block size would also be doubled (which would have changed the consensus rules). Virtually all large service providers and miners were publicly on board, and plans were set in motion to effect the changes. However, a curveball was thrown when a user-led effort prompted the activation of the SegWit network upgrade without changing the network consensus rules and without increasing the block size.¹¹ The effort to change the network's consensus rules failed miserably, and bitcoin steadily marched forward undisturbed. In practice, it often cannot be known whether bitcoin is resistant to various threats until the threats present themselves. In this case, disorder prevented coordinated forces from influencing the network, and everyone learned the extent to which bitcoin was resistant to censorship, further strengthening the network.

This episode in bitcoin's history demonstrated that no one had unilateral control over the network—not even the most powerful companies and miners working in concert could alter bitcoin. It was an incontrovertible demonstration of the network's resistance to censorship. While most participants likely supported the increase in the block size (or at least the idea), it was always a marginal issue. And when it comes to change, bitcoin's default

11. Phil Geiger, "Bitcoin Refuses to Centralize," *Keeping Stock* (blog), Medium, 27 August 2018.

position is no, even for seemingly inconsequential changes. Only an overwhelming majority of all participants (naturally with competing priorities) can change the network's consensus rules. In this instance, it was not really a debate about block size or transaction capacity—but instead whether bitcoin was sufficiently decentralized to prevent external forces from influencing the network and changing the consensus rules. If bitcoin had been susceptible to change by the dictate of a few centralized companies and miners, it would have established that bitcoin was censorable, which is a slippery slope. There would have been no reason to believe that other changes would not be forced upon the network in the future. Ultimately, it would have severely impaired the credibility of bitcoin's fixed 21 million supply.

Before SegWit2x Failure	After SegWit2x Failure
<p>Ted Rogers @tedmrogers</p> <p>To be clearer- we care deeply about censorship resistance. But does avg new user care more about that or Tx fees & speed? I think the latter</p> <p>6 Sep 2017</p>	<p>Ted Rogers @tedmrogers Replying to @cryptoOwl3</p> <p>3/ Ironically, it was the loss of the Segwit2x debate that made me realize all this once and for all - large powerful industry threw everything at implement a seemingly innocuous change to BTC in order to relieve a (perceived) crisis. We lost, badly.</p> <p>4/ the Segwit2x fail was the final victory lap for #bitcoin as digital gold. BTC is uncontrollable, ungovernable, and completely decentralized. Immutable. Agility & governance might help building a currency but its a liability for a store of value and for an immutable record of txs.</p> <p>23 Apr 2018</p>

FIGURE 4.3

The most powerful players in bitcoin colluded, yet failed to co-opt the network because of decentralization. Bitcoin was not just resilient. It emerged stronger as a result. It reinforced bitcoin's long-term viability. The entire network was educated on the importance of censorship resistance and witnessed just how uncensorable bitcoin had become. The lesson informs future behavior as the economic costs and consequences are both real and

permanent. Resources to support the effort became sunk costs, reputations were damaged, and costly trades were made. All said, confidence in bitcoin increased as a function of the failed attempt to control the network, and confidence is not just a passive descriptor. The lessons learned from this attack dissuade future attempts to co-opt the network and drives adoption of bitcoin. Increasing adoption further decentralizes the network, making it more resistant to censorship and outside influence. It may seem like chaos, but social disorder was and will continue to be an asset that secures the network from unpredictable and undesired change.

Bitcoin Benefits from Stressors

Attempts to influence the network consensus rules may be the most acute stressor—as it is these rules that underpin the entire system and create order out of disorder—but bitcoin is consistently exposed to a myriad of smaller stressors that similarly strengthen the network as a whole and over time. There are many different forms of stress, but because bitcoin is exposed to a wide variety of stressors on a consistent basis, the network is forced to constantly adapt and evolve while also building its immune system from the outside in.

Each form of stress hardens the bitcoin network and often for different reasons. Whenever governments take action in an attempt to ban or otherwise restrict the use of bitcoin, the network continues to function unperturbed. With a combined population of 2.7 billion people, the governments of China and India have both taken material actions to curb the spread of bitcoin. Despite this, the network continues to function without flaw, and the use of bitcoin continues in both countries. After the Reserve Bank of India restricted the ability of banks to service bitcoin or cryptocurrency-related companies, the Supreme Court of India eventually overturned the ban as unconstitutional. It set a precedent in more ways than one. First, the central bank was overruled. Second, the ban was ultimately unsuccessful as people continued to find ways to access bitcoin. Third, the network was unfazed despite these actions.

Stressor	Example	Impact / Outcome
Consensus rules	<ul style="list-style-type: none"> • SegWit2x civil war • Bitcoin Cash hard fork 	<ul style="list-style-type: none"> • Bitcoin proves to be censorship-resistant • Bitcoin wins, strengthens
Government action	<ul style="list-style-type: none"> • India's central bank banning banks' ability to service bitcoin companies • China clamping down on exchanges and mining activities • US Congress representatives calling for bans or restrictions • Bitcoin addresses placed on OFAC list 	<ul style="list-style-type: none"> • Network continues to function uninterrupted • Network adapts and immunizes threat • Bitcoin wins, strengthens
Competing protocols	<ul style="list-style-type: none"> • Bitcoin hard forks and copies • "World Computer" • Utility tokens • Stablecoins • Facebook's Libra 	<ul style="list-style-type: none"> • Competing currencies fail • Bitcoin remains dominant • Market tests provide information • Bitcoin wins, strengthens
Company or service provider error	<ul style="list-style-type: none"> • Mt. Gox hack (stolen bitcoin) • Bitfinex hack (stolen bitcoin) • Binance hack (stolen bitcoin) • BlockFi hack (stolen personal information) • Hardware wallet vulnerabilities 	<ul style="list-style-type: none"> • Errors owned by responsible parties • No bailouts • Accountability eliminates moral hazard • Companies adapt or fail • Bitcoin wins, strengthens
Individual user error	<ul style="list-style-type: none"> • Individual exchange accounts hacked • Accounts frozen or terminated • SIM swaps • Bitcoin wallets lost or stolen • Forgotten passphrases to private keys • Malicious browser extensions or malware 	<ul style="list-style-type: none"> • Errors owned by responsible parties • No bailouts • Accountability eliminates moral hazard • Individuals adapt or lose money • Bitcoin wins, strengthens

The figure consists of two separate news articles from Bloomberg, each enclosed in a thin black border. The top article is titled "Cryptocurrency Virtually Outlawed in India as Top Court Backs Ban" and is categorized under "Cryptocurrencies". It was written by Upmanyu Trivedi and Rahul Satija, published on July 3, 2018, at 4:10 AM CDT, and updated on July 3, 2018, at 5:55 AM CDT. The bottom article is titled "Cryptocurrency Bourses Win India Case Against Central Bank Curbs" and is categorized under "Technology". It was also written by Upmanyu Trivedi, published on March 3, 2020, at 11:27 PM CST, and updated on March 4, 2020, at 1:41 AM CST.

FIGURE 4.4

Source: Bloomberg

Separately, China has taken measures to restrict the ability of exchanges to facilitate bitcoin trading and has expressed an interest in eliminating bitcoin mining. As they do in India, people continue to use bitcoin in China with no disruption to the network. Naturally, as government regulation in China has become more restrictive, miners have begun to look to more stable jurisdictions. Bitcoin mining in the United States (among other regions) continues to grow, with Peter Thiel recently backing a startup building out mining operations in West Texas.¹² Regardless of the threat, bitcoin exists beyond countries (and governments). The network organically adapts to jurisdictional risks and continues to function without interruption. As network participants observe the failed attempts to inhibit bitcoin's growth and witness how it adapts, bitcoin does not merely remain static. It actually becomes more resilient through this process by routing around and immunizing each passing threat.

An entirely different type of stress comes in the form of competing cryptocurrencies. There have been thousands of variations following bitcoin's launch in 2009, often espousing different purposes and "use cases." In reality, every single one has been competing with bitcoin as money (whether

12. Jeff John Roberts, "Texas Bitcoin Mining Startup Gets \$50 Million From Peter Thiel to Steal China's Crypto Crown," *Fortune*, 15 October 2019.

it is realized or not). Creators will call out perceived flaws in bitcoin and explain how their competing protocol intends to improve on its “limitations.” However, despite thousands of competitors, bitcoin accounts for ~70% of all cryptocurrencies in terms of market value. And when adjusted for liquidity, the estimate is closer to ~90%. Meaning thousands of competing cryptocurrencies account for 10% to 30%.

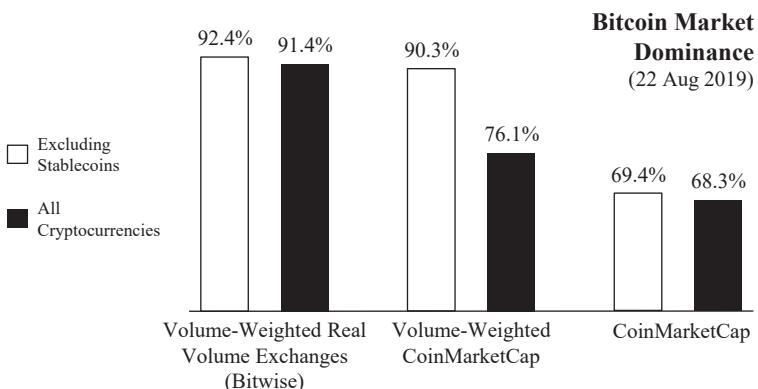


FIGURE 4.5
Source: Arcane Research

That is the market distinguishing between bitcoin and the field. Competition is inherently good for bitcoin. Not only does each attempt to create a better bitcoin fail, but the repeated failures inform market participants that there is something that differentiates bitcoin. Even if the reason is not immediately self-evident, the market still provides valuable information. Bitcoin does not just withstand the competition. It beats the competition. The market test teaches people that bitcoin cannot be copied better than any amount of reason and logic can. Through the failed experiences of competing currencies, bitcoin accumulates more human capital and a larger holder base, with the network growing as a direct result. If bitcoin were never tested or challenged, it would not have the opportunity to benefit from stress.

While external threats to the network create positive externalities, bitcoin also benefits from more frequent and consistent internal stressors, such

as malicious attacks or unintentional errors. Attacks aimed at participants (whether an individual or company) occur at a near-constant clip. Each participant is maximally and independently responsible for the security of their bitcoin holdings, whether choosing to trust a third party or directly assuming that responsibility. Many of the largest exchanges in the world have been hacked, as have numerous individuals within the network. For those that have not, the threat always exists. As participants are compromised, hacked, or otherwise have access to their bitcoin restricted, it does not impact the functioning of the network. But like all stressors, the threats directly cause the network to adapt to these vectors and become stronger.

“Your keys, your bitcoin. Not your keys, not your bitcoin.”

—Andreas Antonopoulos,
on the lessons from the 2016 Bitfinex hack¹³

Pirate Beachbum @piratebeachbum

Friend just called and his sim card was cloned and they cleaned out his coinbase account and tried to transfer his savings account to coinbase. I told him a year ago not to leave any Bitcoin on coinbase. Very few listen!

25 May 2020



FIGURE 4.6

With each critical exchange failure or hack, market participants increasingly shift to taking on the responsibility of holding their own bitcoin, independent of third-party service providers. The same is true in response to individual accounts at exchanges getting hacked. Similarly, as threats are identified by those who secure their own bitcoin, more secure wallets are developed, and users opt toward methods that reduce or eliminate single points of failure. Because everyone is personally accountable and no cost of error can

13. Olusegun Ogundehi, “Antonopoulos: Your Keys, Your Bitcoin. Not Your Keys, Not Your Bitcoin,” Cointelegraph, 10 August 2016.

be socialized, the incentive structure dictates that participants constantly seek out better ways of securing bitcoin. It is a constant evolution born out of the reality that stressors exist everywhere. The network is not exposed to critical failures because the entire universe of market participants iterates through trial and error around the clock and at every level. Open competition and endless market opportunities incentivize innovation—the network benefits as a whole, strengthening naturally and organically.

Bitcoin Benefits from Volatility

Similar to the benefit provided by consistent stressors, volatility tangibly builds the system's immunity. While often lamented as a critical flaw, volatility is a feature, not a bug. Volatility is price discovery, and in bitcoin, it is unceasing and uninterrupted. There are no Fed market operations to rescue investors, nor are there circuit breakers. Everyone is individually responsible for managing volatility, and there is no one to offer bailouts. Moral hazard is eliminated network wide. In a world without bailouts, the market function of price discovery is far truer because external forces cannot directly manipulate it. Through experience, market participants quickly learn how unforgiving volatility can be. It is akin to a child touching a hot stove, a mistake that will likely only happen once. And should the lesson go unheeded, the individual is sacrificed to benefit the whole. There is no “too big to fail” in bitcoin. Ultimately, price communicates information. All participants independently observe and navigate market forces, either adapting or individually paying the price.

However, information is not just communicated through price volatility. Volatility is also how bitcoin gets distributed. Every bitcoin sold is a bitcoin bought. Consistently over time, the ownership of the network becomes more decentralized, and bouts of volatility result in greater distribution with large volumes of the currency changing hands. As the network becomes more decentralized, it similarly becomes more censorship-resistant. As each individual within the network holds a smaller and smaller share of

the currency (on average) over time, it results in a dynamic where price is decreasingly dependent on the preferences of a few large holders. This is not to say that there are no large holders remaining that can singularly influence price and volatility. But as a directional trend, any individual participant's impact on price diminishes over time, often directly through the distributive function of volatility. In very tangible ways, volatility strengthens bitcoin.

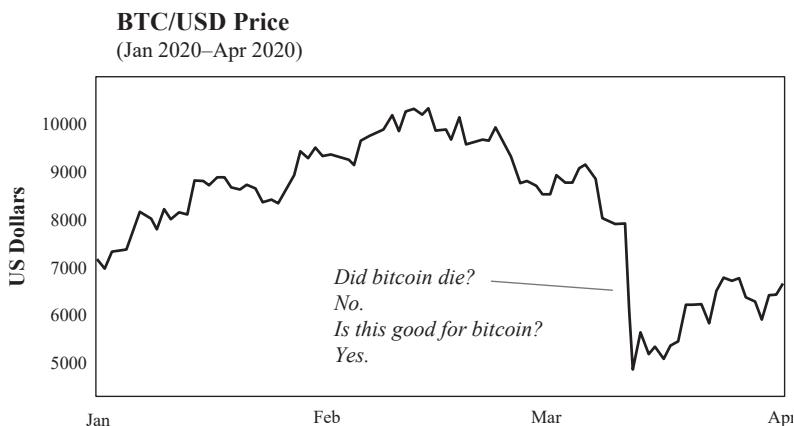


FIGURE 4.7
Price Source: Bitstamp

When network participants, individually and as a whole, observe bitcoin's continued survival, especially following extreme downside volatility, confidence in the network strengthens. At some price, individuals are willing to step in and catch the falling knife. Through these episodes, bitcoin accumulates more human capital. The weak hands get shaken out, but the strongest hands survive (often in the form of new holders), causing the network to become more resilient. Bitcoin does not merely remain static or simply absorb the disruption. It actively feeds on the chaos. In the end, near-term volatility directly contributes to long-term stability. By maintaining a fixed supply with highly variable present demand, the market performs price discovery twenty-four hours a day, seven days a week. The intermittent stress trains and hardens all individual owners, which prevents the network

from being exposed to systemic risk. All the while, the opposite is true of fiat currencies. Central banks maintain short-term stability by suppressing volatility. The consequence is the accumulation of imbalances below the surface, leading to fragility. These policies all but ensure more severe systemic shocks in the long term, as has been witnessed with increasing regularity over the last two decades. Volatility in bitcoin benefits participants by communicating information with the least distortion. The contrast between the two competing systems could not be more extreme. Without volatility today, long-term stability would not be possible.

Complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks. [...] Such environments eventually experience massive blowups, catching everyone off-guard and undoing years of stability.

Variation is information. When there is no variation, there is no information [...] there is no freedom without noise—and no stability without volatility.

—Nassim Taleb and Mark Blyth¹⁴

Bitcoin Benefits from Randomness

Many of the greatest things man has achieved are the result not of consciously directed thought, and still less the product of a deliberately coordinated effort of many individuals, but of a process in which the individual plays a part which he can never fully understand. They are greater than any individual precisely because they result from the combination of knowledge more extensive than a single mind can master.

—Friedrich A. Hayek¹⁵

14. Nassim N. Taleb and Mark Blyth, “The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous,” *Foreign Affairs* 90, no. 3 (May/June 2011).

15. Friedrich A. Hayek, *The Counter-Revolution of Science: Studies on the Abuse of Reason* (Glencoe, IL: Free Press, 1952), 84–85.

While most people recognize that there is intelligent design in bitcoin's foundation, the element of randomness in its evolution is often overlooked. What bitcoin has evolved to become (money) is largely a function of that randomness. Lightning was caught in a bottle. It resulted from thousands of people making thousands of independent decisions very early on—a process that continues to this day—from cryptographers and developers contributing time and energy to companies and investors building infrastructure to users just wanting to find a better way to store value. If someone magically pressed a reset button going back to 2008, when the bitcoin white paper was published, and the same initial code were released, placing the same people in the same rooms, bitcoin would very likely not be what it is today. It may be “better” or “worse,” but ultimately, bitcoin was and continues to be a product of randomness. It is not the product of consciously directed or controlled thought, and it expands beyond the resources of individual minds because of that fact. For those who perceive flaws in bitcoin and have (or had) ideas of how to improve upon it, the intelligence of bitcoin's design is often observed and acknowledged. While you can copy the design and change individual features, you cannot replicate the conditions and subsequent randomness.

One week after the launch of bitcoin, Hal Finney famously tweeted to the world that he was “running bitcoin,” becoming the first known person to join the network after its launch. In 2011, Ross Ulbricht was alleged to have created the Silk Road marketplace. This website ultimately leveraged bitcoin to facilitate online payments for drugs, establishing one of the earliest widespread uses of bitcoin in commerce and undoubtedly playing a material role in expanding early adoption and awareness. In 2014, the Tokyo-based bitcoin exchange Mt. Gox was hacked, and that event may have had the single greatest influence on the advancement and proliferation of bitcoin hardware wallets as individuals and companies looked to eliminate the risks posed by third-party exchanges. In 2017, after a bitcoin service provider drew the ire of Nicolas Dorier, he set out to build a product that would obsolete that provider and service, spawning one of the most exciting open-source projects within bitcoin, the self-hosted payment processor BTCPay Server.

halfin @halfin

Running bitcoin

10 Jan 2009



FIGURE 4.8

Nicolas Dorier @NicolasDorier

Replies to @BitPay

This is lies, my trust in you is broken, I will make you obsolete

17 Aug 2017



FIGURE 4.9

In 2018, Saifedean Ammous released the book *The Bitcoin Standard*, which has accelerated knowledge distribution and contributed to a wave of bitcoin adoption. There are obviously too many random acts to count or acknowledge. Still, the randomness derived from bitcoin's permissionless nature, lacking any conscious control, allowed it to evolve into the antifragile system it is today. Bitcoin would have never been viable as a currency if it was under the direction of any single individual, company, or country. If it had been, bitcoin would have always been dependent on trust and would have lacked the randomness necessary to create a system capable of dispensing with the need for conscious control. Randomness is irreplicable, and the foundation of bitcoin was built on it.

Bitcoin Is Antifragile

In aggregate, bitcoin benefits from disorder as both a currency and economic system. The constant exposure to stressors, volatility, and randomness causes bitcoin to evolve and adapt. It ultimately becomes stronger in a near-uniform fashion and in a way that would not be possible in the absence of disorder. Bitcoin may still be young, but it is not temporary. It was released into the wild, and a system has spawned that cannot be controlled or shut down. Like an elusive ghost, it is both everywhere and nowhere simultaneously. Its decentralized and permissionless nature eliminates single points of failure and incentivizes innovation, ultimately ensuring both its survival and a constant strengthening of its immune system as a function of time, trial, and error.

Beyond resilient, bitcoin does not just absorb shocks. It gets better as a direct result. While it is easy to fall into the trap of believing bitcoin to be untested, unproven, and not permanent, it is precisely the opposite. Bitcoin has been tested constantly for twelve years (as of the time of writing), each time not only proving it was up to the challenge but emerging in a stronger state. At the end of the day, bitcoin is more permanent than risky because of its antifragility. As a currency system, it manages to extend the utilization of resources beyond the control of deliberately coordinated effort, entirely dispensing with the need for conscious control. Bitcoin is the antifragile competitor to the inherently fragile legacy monetary system. The legacy system is crippled by moral hazard and is dependent on trust and centralized control. Imbalances accumulate when exposed to stress and disorder, principally as a function of trillions in bailouts with each passing shock, further weakening its immune system and increasing its fragility. In contrast, bitcoin is a system devoid of moral hazard and operates flawlessly on a decentralized basis, without trust or bailouts. It eliminates imbalance and sources of fragility as a constant process, further strengthening the currency system as a whole. What doesn't kill the legacy monetary system only makes it weaker. What doesn't kill bitcoin only makes it stronger.

But those who clamor for “conscious direction”—and who cannot believe that anything which has evolved without design (and even without our understanding it) should solve problems which we should not be able to solve consciously—should remember this: The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore, how to dispense with the need of conscious control, and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do.

—Friedrich A. Hayek¹⁶

16. Friedrich A. Hayek, “The Use of Knowledge in Society,” *American Economic Review* 35, no. 4 (September 1945): 527.

CHAPTER FIVE

Bitcoin Is the Great Definancialization

*(Originally published on 23 December 2020
in The Bitcoin Times, Edition 3)*

Engineered Decay

Have you ever had a financial advisor, or maybe even a parent, tell you that you need to make your money grow? This idea has been so hardwired into the minds of hard-working people all over the world that it has become practically second nature to the very idea of work.

The line has been repeated so many times that it is now a de facto part of working culture. Get a salaried position, max out your 401(k) contribution (maybe your employer matches 3%!), select a few mutual funds with catchy marketing names, and watch your money grow. Most folks navigate this path on autopilot every two weeks, never questioning the wisdom nor being conscious of the risks. It is just what “smart people” do. Many now associate the activity with savings, but in reality, financialization has turned retirement savers into perpetual risk-takers. The consequence is that investing has become a second full-time job for many, if not most.

Financialization has been so errantly normalized that the lines between saving (not taking risk) and investing (taking risk) have become blurred to the extent that most people think of the two activities as being one and the same. Believing that financial engineering is a necessary path to a happy retirement might lack common sense, but it has become conventional wisdom.

MAKE YOUR MONEY GROW



Or maybe you just need a better form of money?

Over the course of the last several decades, economies have become increasingly financialized, particularly in the developed world (and specifically the US). Increased financialization has become the necessary companion to the idea that you must make your money grow. But the idea itself only emerged in the mainstream consciousness as everyone similarly became conditioned to the unfortunate reality that money loses its value over time.

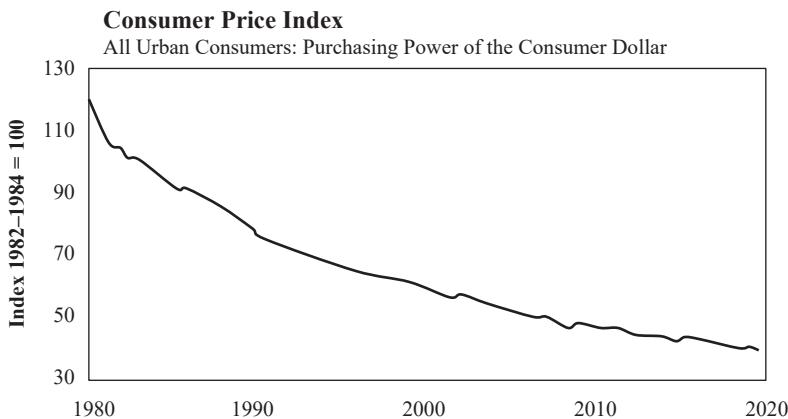


FIGURE 5.1
Source: US Bureau of Labor Statistics

*Money Loses Value → Need to Make Money Grow →
Need Financial Products to Make Money Grow → Repeat.*

The extent to which the need even exists is largely a function of money losing its value over time. That is the starting point, and the most unfortunate part is that central banks intentionally engineer this outcome. Most global central banks target the devaluation of their local currencies by approximately 2% per year and do so by increasing the money supply. How or why is less relevant. It is a reality, and there are consequences. Rather than simply being able to save for a rainy day, future retirement funds are invested and put at constant risk, often just as a means to keep up with the very inflation manufactured by central banks.

Central banks perversely drive the demand function for such investments by devaluing money. An overfinancialized economy is the logical conclusion of monetary inflation, and it has induced perpetual risk-taking while disincentivizing savings. A system that disincentivizes saving and forces people into a position of risk-taking creates instability, and it is neither productive nor sustainable. It should be obvious to even the untrained eye that the overarching force driving the trend toward financialization, and financial engineering more broadly, is the broken incentive structure of the monetary medium that underpins all economic activity.

At a fundamental level, there is nothing inherently wrong with joint-stock companies, bond offerings, or any pooled investment vehicle for that matter. While individual investment vehicles may be structurally flawed, there can be (and often is) value created through pooled investment vehicles and capital allocation functions. Pooled risk is not the issue, nor is the existence of financial assets. Instead, the fundamental problem is the degree to which the economy has become financialized as an unintended consequence of otherwise rational responses to a broken and manipulated monetary structure.



FIGURE 5.2

What happens when hundreds of millions of market participants realize that their money is artificially, yet intentionally, engineered to lose 2% of its value every year? It is either accept the inevitable decay or try to keep up with inflation by taking incremental risk, and the overwhelming majority of people have been conditioned to the latter. The consequence is that money must be invested, meaning it must be put at risk of loss. Because monetary debasement never abates, this cycle persists. Essentially, people take risk in their day job and are then trained to put any money they do manage to save right back at risk, just to keep up with inflation, if nothing more. It is the definition of a hamster wheel—running hard just to stay in the same place. It may be absurd, but this is the present reality. And it is not without consequence.

Savings vs. Risk

While the relationship between savings and risk is often misunderstood, risk must be taken in order for any individual to accumulate savings in the first place. Risk comes in the form of dedicating time and energy to some pursuit that others value (and must continue to value) in order to be compensated (and continue to be compensated). It starts with education, training, and ultimately perfecting a craft over time that others value. That is risk-taking.

Investing time and energy in an attempt to earn a living and to produce value for others requires accepting high degrees of future uncertainty. If successful, it ends with a classroom of students, a product on a shelf, a world-class performance, a full day of hard manual labor, or anything else that others value. The risk is taken on the front end with the hope and expectation that someone else will compensate you for your time spent and value delivered.

Compensation typically comes in the form of money because money, as an economic good, allows individuals to convert their own value into a wide range of value created by others. In a world in which money is not manipulated, monetary savings would best be described as the difference between the value one has produced for others and the value one has consumed from others. Savings is simply consumption or investment deferred into the future. Said another way, savings represents the excess of what one has produced but not yet consumed. That, however, is not the world that exists today. With modern money, there is a fly in the ointment.

Central banks create more and more money, which causes savings to be perpetually devalued. The entire incentive structure of money is manipulated, including the integrity of the scorecard that tracks who has created and consumed what value. Any value created today is ensured to purchase less in the future as central banks arbitrarily allocate more units of the currency. Money is intended to store value, not lose value. But with monetary economics engineered by central banks, everyone is unwittingly forced into the position of taking risk as a means to continuously replace savings as it is debased. Rather than benefiting from risks already taken, everyone is forced to take incremental risk.

Forcing risk-taking on practically all individuals within an economic system is not natural, nor is it fundamental to the functioning of an economy. It is precisely the opposite, and it is detrimental to the stability of the system as a whole. As an economic function, risk-taking itself is productive, necessary, and inevitable. The unhealthy part is specifically when individuals are forced (consciously or not) into taking risk as a byproduct of central banks manufacturing money to lose value. Risk-taking is productive when

it is intentional, voluntary, and undertaken in the pursuit of accumulating capital. While deciphering between productive investment and that which is induced by monetary inflation is inherently gray, you know it when you see it. Productive investment occurs naturally as market participants work to improve their own lives and the lives of those around them. The incentives to take risk in a free market already exist. There is nothing to be gained, and a lot to lose, through central bank intervention.

Nic Carter @nic_carter

Replies to @GeorgeSelgin

Stocks of course are treated as savings devices, so yes. They have moneyness.

30 Nov 2020



Pierre Rochard @pierre_rochard

Replies to @nic_carter

IMO stocks became a monetary instrument because inflation pushed savers out of USD, then it pushed them out of CDs and money market funds, then it pushed them out of bonds, now the responsible thing to do is to use MSFT and/or low cost index funds for saving instead of investing.

30 Nov 2020



FIGURE 5.3

Risk-taking becomes counterproductive when it is born more out of a hostage-taking situation than free will. That should be intuitive. But it is exactly what occurs when investment is induced by monetary debasement. Recognize that 100% of all future investment (and consumption, for that matter) comes from savings. Manipulating monetary incentives and specifically creating a disincentive to save merely distorts the timing and terms of future investment. It forces the hand of savers everywhere and unnecessarily lights a shortened fuse on all monetary savings. It inevitably creates a game of hot potato, with no one wanting to hold money because it loses value when the opposite should be true. What kind of investment do you think a

world like this would produce? The melting ice cube that is central bank currency has induced a cycle of perpetual risk-taking, whereby the majority of all savings are almost immediately put back at risk and invested in financial assets. This occurs either directly at the hands of an individual or indirectly by a deposit-taking financial institution. Made worse, the two operations have become so confused and conflated that most people consider investments, particularly those in financial assets, as savings.

Without question, investments (in financial assets or otherwise) are not the equivalent of savings, and there is nothing normal or natural about risk-taking induced by the disincentive to save created by central banks. Anyone with common sense and real-world experience understands that. Still, it doesn't change the fact that money loses its value every year (because it does), and knowledge of that fact very rationally dictates behavior. Everyone has been forced to accept a manufactured dilemma. The idea that you must make your money grow is one of the greatest lies ever told. It isn't true at all. Central banks have created that false dilemma. The greatest trick that central banks ever pulled was convincing the world that individuals must perpetually take risk just to preserve value already created (and saved). It is insane, and the only practical solution is to find a better form of money that eliminates the negative asymmetry inherent to systemic currency debasement. That is what bitcoin represents. A better form of money that provides all individuals with a credible path to opt out and get off the hamster wheel.

The Great Financialization

Whether one considers the game to be inherently rigged or simply acknowledges the reality of persistent monetary debasement, economies everywhere have been forced to adapt to a world in which money loses its value. While the intention is to induce investment and spur growth in aggregate demand (i.e., the total demand for goods and services within an economy), there are always unintended consequences when economic incentives become manipulated by exogenous forces. Even the greatest cynic probably wishes that the

world's problems could be solved by printing money. However, rather than print money and have problems magically disappear, the proverbial can has just been kicked further and further down the road. Economies have been structurally and permanently altered as a function of money creation.

The Fed may have thought it could print money as a means to induce productive investment, but what it actually produced was malinvestment and a massively overfinancialized economy. Economies have become increasingly financialized as a direct result of monetary debasement and a manipulated cost of credit, which was an intended derivative of monetary debasement. One would have to be blind not to see the causal and interconnected relationship—a money manufactured to lose its value, a disincentive to hold money, artificially cheap credit, and the rapid expansion of financial assets, including debt instruments within the credit system.

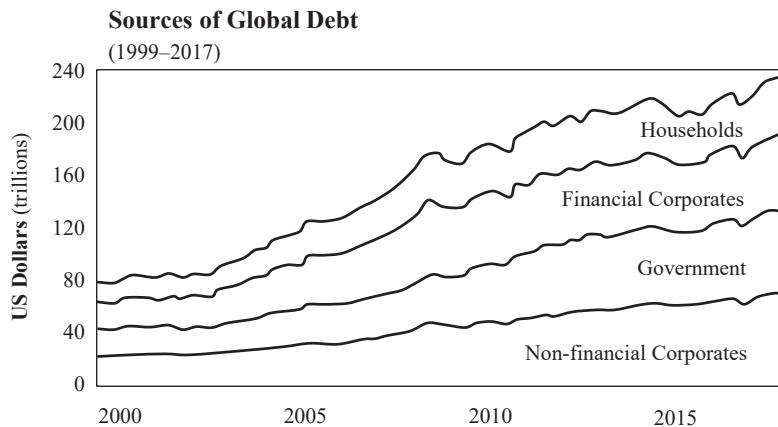
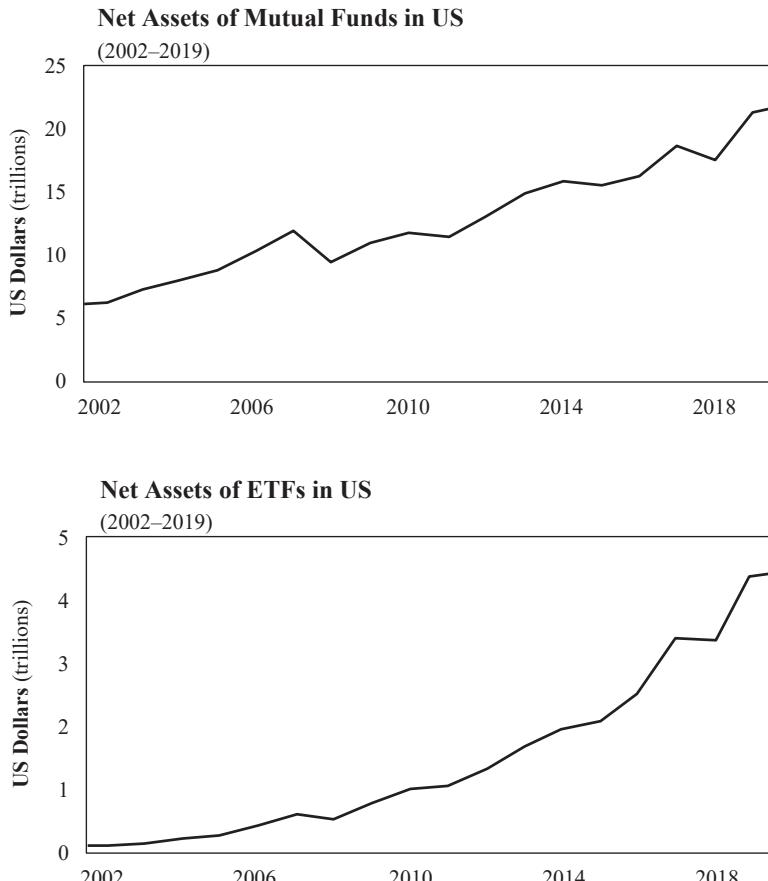


FIGURE 5.4
Source: Institute of International Finance

The banking and wealth management industries have metastasized by this same function. It is like a drug dealer who creates his own market by giving the first hit away for free. Drug dealers create their own demand by getting the addict hooked. The dynamic is similar between the Fed and financialization via monetary debasement. The Fed created a problem, and

then a treatment for the problem was necessary. By manufacturing money to lose value, markets for financial products emerged that otherwise would not. Products have been created to help people financially engineer their way out of the very hole created by the Fed. The need arises to take risk in an attempt to produce returns to replace what is lost via monetary inflation.

**FIGURES 5.5 & 5.6**

Source: Statista.com

The financial sector has captured a larger percentage of the economy over time because there is greater demand for financial services in a world in

which money cannot reliably be expected to store value. Stocks, corporate bonds, treasuries, sovereign bonds, mutual funds, equity ETFs, bond ETFs, leveraged ETFs, triple leveraged ETFs, fractional shares, mortgage-backed securities, CDOs, CLOs, CDS, CDX, synthetic CDS/CDX, etc.—all of these products represent the financialization of the economy, and they become more relevant (and in greater demand) when the monetary function is broken.

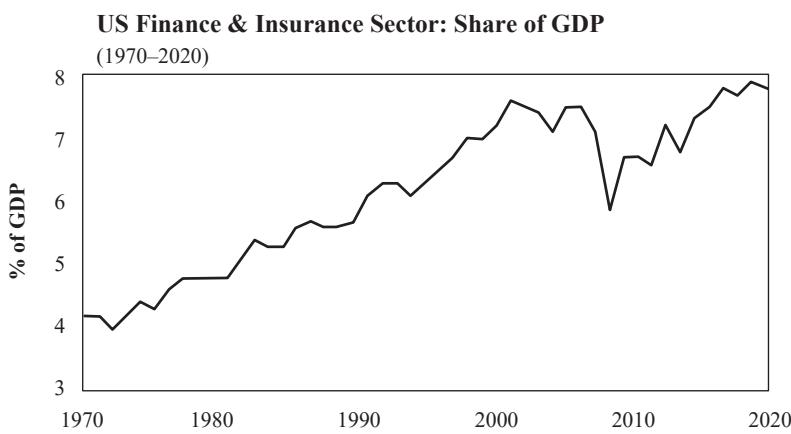


FIGURE 5.7

Source: Federal Reserve Economic Data (FRED), US Bureau of Economic Analysis

Each incremental shift to pool, package, and repackage risk can be tied back to an intentionally broken monetary incentive structure and the manufactured need to make money grow. Again, this is not to say that certain financial products or capital structures do not create value. Instead, the problem is the *degree* to which financial products are utilized and the extent to which risk has been layered on top of risk, resulting from the broken monetary incentives.

While the vast majority of all market participants have been lulled to sleep as the Fed has normalized an annual inflation target of 2%, consider the consequence of that policy over a decade or two decades. It represents a compounded 20% and 35% loss of monetary savings over ten or twenty

years, respectively. What would one expect to occur if an entire society, individually and collectively, were put in the position of needing to recreate or replace 20% to 35% of their savings just to stay in the same place or get back to even?

The aggregate impact is massive widespread malinvestment: investment in activities that would not have occurred if people were not forced into a position of taking ill-advised risk merely to replace the expected future loss of current savings. At an individual level, it's the doctor, nurse, engineer, teacher, butcher, grocer, or builder turned financial investor, plowing the majority of their savings into Wall Street financial products that bear risk while perceiving there to be none. Over time, stocks only go up, real estate only goes up, and interest rates only go down.

Dave Portnoy @stoolpresidente

Say it with me... Stocks only go up. Only losers take profits.
#DDTG



4 Jun 2020

FIGURE 5.8

How or why is a mystery to the Davey Day Traders of the world (for the record, the author is a Dave Portnoy fan), and it matters not. It is just how the world is perceived to work, and everyone acts accordingly. Rest assured. It will all end badly. Most individuals have come to believe that investments in financial assets are just a better (and necessary) way to save,

which dictates behavior. A “diversified portfolio” has become so synonymous with savings that it is neither perceived to bear risk nor associated with actively taking risk. While this couldn’t be further from the truth, the choice is either to take risk via financial investments or to leave savings in a monetary medium that is sure to purchase less and less in the future. It is an unnerving game that everyone is forced to play. It is where “damned if you do” meets “damned if you don’t.”

Consequences of a Disincentive to Save

A negative feedback loop exists in a world where money is engineered to lose value by design. By eliminating the very possibility of saving money as a winning proposition, all outcomes skew far more negative in aggregate. Just holding money is a losing hand by default. So is perpetual risk-taking as a forced substitute. Effectively, all hands become losing hands when the possibility of winning by saving money is removed. Recall that each individual possessing money has already taken risks to get it in the first place. A positive incentive to save (and not invest) is not equivalent to rewarding people for not taking risk. It is quite the opposite. It is rewarding people who have already taken risk with the option of merely holding money without the express promise of its purchasing power declining in the future.

In a free market, money might increase or decrease in value over a particular time horizon. But *guaranteeing* that money will lose value creates an extremely negative outcome where the majority of participants within an economy lack actual savings. Because money loses its value, opportunity cost is often believed to be a one-way street: spend your money now because it will purchase less tomorrow. The very idea of holding cash (formerly known as saving) has been conditioned in mainstream financial circles to be a near-crazy proposition. How crazy is that? While money is intended to store value, no one wants to hold it because today’s predominant currencies do the opposite. Rather than seek out a better form of money, everyone just invests instead!

“I still think that cash is trash relative to other alternatives, particularly those that will retain their value or increase their value during reflationary periods.”

—Ray Dalio, April 2020¹⁷

Even the most revered Wall Street investors are susceptible to getting caught up in the madness and can act a fool. Risk-taking for inflation’s sake is no better than buying lottery tickets, but that is the consequence of creating a disincentive to save. Economic opportunity cost becomes harder to measure and evaluate when monetary incentives are broken. Today, purchasing financial assets is rationalized merely because the dollar is expected to lose its value. But the consequence extends far beyond savings and investment. Every economic decision becomes impaired when money is not fulfilling its intended purpose of storing value.

All spending versus savings decisions, including day-to-day consumption, become negatively biased when money persistently loses value. By reintroducing a more explicit opportunity cost to spending money (i.e., an incentive to save), everyone’s risk calculus necessarily changes. Every economic decision becomes sharper when money fulfills its proper function of storing value. When a monetary medium can be credibly expected at minimum to maintain its value, if not increase, every spend-versus-save decision becomes more focused and is made with greater scrutiny when governed and informed by a better-aligned incentive structure.

“One of the greatest mistakes is to judge policies and programs by their intentions rather than their results.”

—Milton Friedman¹⁸

17. Ray Dalio, “I’m Ray Dalio—Founder of Bridgewater Associates and Author of *Principles: Life & Work*. Ask Me Anything,” Reddit, r/IamA, 7 April 2020.

18. Milton Friedman, “Living Within Our Means,” interview by Richard D. Heffner, *Open Minds*, PBS, 7 December 1975.

Keynesian economists fear such a world, believing that investments would not be made if an incentive to save existed. The flawed theory asserts that if people are incentivized to “hoard” money, no one will ever spend money, and “necessary” investments will not be made. If no one spends and risk-taking investments are not made, unemployment will rise! It truly is an economic theory reserved for the classroom. While counterintuitive to Keynesians, risk *will* be taken and money will be spent in a world that incentivizes savings.

Not only that, but the quality of consumption and investment will both benefit from undistorted price signals and with the opportunity cost of money more clearly priced by a free market. When all spending decisions are evaluated against the expectation of potentially greater purchasing power in the future (rather than less), investments will be steered toward the most productive activities, and day-to-day consumption will be filtered with greater scrutiny.

Conversely, when the decision point of investment is heavily influenced by an aversion to holding dollars, the result is financialization. Similarly, when consumption preferences are guided by the expectation that money will lose its value rather than increase in value, investments are made that cater toward those distorted preferences. Short-term incentives beat out long-term incentives. Incumbents are advantaged over new entrants, and the economy stagnates, which fuels financialization, centralization, and financial engineering rather than productive investment. It is cause and effect, intended behavior with unintended but predictable consequences.

Make money lose its value, and people will do dumb shit because doing dumb shit becomes more rational (if not encouraged). People who would otherwise be saving are forced to take incremental risk because their savings are losing value. In that world, savings become financialized. And when you create a disincentive to save, do not be surprised to wake up in a world where very few people have savings. It is exactly what has happened. Although it may astound a tenured economics professor, the general lack of savings induced by the disincentive to save is very predictably a major source of the

inherent fragility in the legacy financial system. Without savings, very few are prepared for any modicum of future uncertainty.

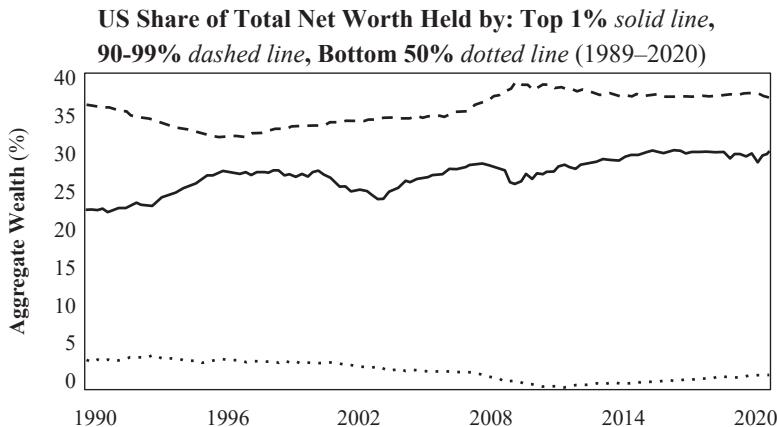


FIGURE 5.9
Source: Federal Reserve Economic Data (FRED)

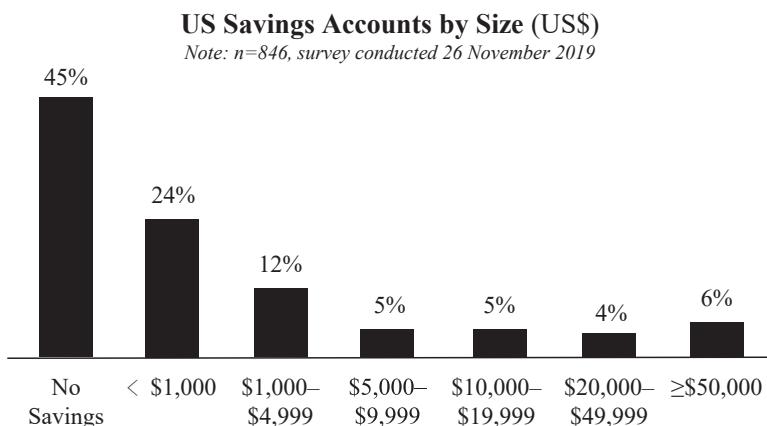


FIGURE 5.10
Source: Statista.com

The Paradox of a Fixed Money Supply

The lack of savings and economic instability that follows is all driven by the broken incentive structure of the underlying currency, and this is the principal problem that bitcoin fixes. By eliminating the possibility of monetary debasement, incentives that were broken become aligned. There will only ever be 21 million bitcoin, and that alone is sufficiently powerful to begin to reverse the trend of financialization. While each bitcoin is divisible into 100 million units (or to eight decimal places), the nominal supply of bitcoin is capped at 21 million. Bitcoin can be further divided into smaller and smaller units as more and more people adopt it as a monetary standard, but no one can arbitrarily create more bitcoin. Consider a terminal state in which all 21 million bitcoin are in circulation. Technically, no more than 21 million bitcoin can be saved, but the consequence is that 100% of all bitcoin is always being saved—by someone at any particular point in time. Bitcoin (including fractions thereof) will transfer from person to person or company to company, but the total supply will be static and perfectly inelastic.

With a fixed money supply, no more or no less money can be saved in aggregate. However, the incentive and propensity to save increases measurably at an individual level as a result. It is a paradox. If more money cannot be saved in aggregate, more people will save on an individual basis. While it may appear to be a simple statement that individuals value scarcity, it serves more as an explanation that an incentive to save *creates* savers. And for someone to save, someone else must spend existing savings. After all, all consumption and investment come from savings. The incentive to save creates savers, and the existence of more savers results in more people with the means to consume and invest. At an individual level, if someone expects a monetary unit to increase in purchasing power, they may reasonably defer either consumption or investment to the future (the keyword being “defer”). That is the incentive to save creating savers. It does not eliminate consumption or investment. It merely ensures that the decision is evaluated with greater scrutiny when future purchasing power is expected to increase.

Imagine every single person simultaneously operating with that as an incentive mechanism, compared to the opposite that exists today.

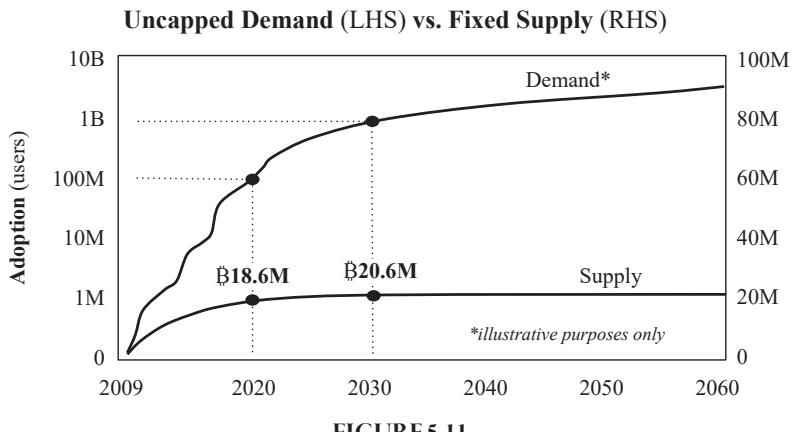


FIGURE 5.11

While Keynesians worry that an appreciating currency will disincentivize consumption and investment in favor of savings—to the detriment of the economy at large—the free market actually works better in practice than it does when applying flawed Keynesian theory. An appreciating currency will be used every day to facilitate consumption and investment because there is an incentive to save, not despite that fact. Everyone is always trying to earn everyone else's money, and everyone still needs to consume real goods every day.

The concept of time preference is described at length in *The Bitcoin Standard* by Saifedean Ammous (2018). While the book is a must-read and no summary can do it justice, a key idea it puts forward is that of time preference. While individuals can have a lower time preference (weighting the future over the present) or a higher time preference (weighting the present over the future), everyone has a positive time preference. As a tool, money is merely a utility in coordinating the economic activity necessary to produce the things that people value and consume in their daily lives. Given that time is inherently scarce and that the future is uncertain, even those

who plan and save for the future (i.e., possessing a low time preference) are predisposed to value the present over the future on the margin. Taken to an extreme for illustrative purposes, if you earned money and literally never spent a dime (or a sat), the money would not have done you any good. Even if the value of money is increasing over time, consumption or investment in the present has an inherent bias over the future, on average, because of positive time preference and daily consumption needs that must be satisfied for survival (if not for want).

$$\begin{aligned} & 7+ \text{Billion People Competing} + 21 \text{ Million Bitcoin} \\ & = \text{Appreciating Currency} + \text{Constant Spending} \end{aligned}$$

Now imagine this principle applied to everyone simultaneously and in a world of bitcoin with a fixed money supply. Seven billion-plus people and only 21 million bitcoin. Everyone has both an incentive to save because there is a finite amount of money and a positive time preference with daily consumption needs. In this world, there would be fierce competition for money. Each individual would have to produce something sufficiently valuable in order to entice someone else to part with their hard-earned money. The roles would then reverse, and the cycle would repeat because it would be the only way to get money. That is the contract bitcoin provides.

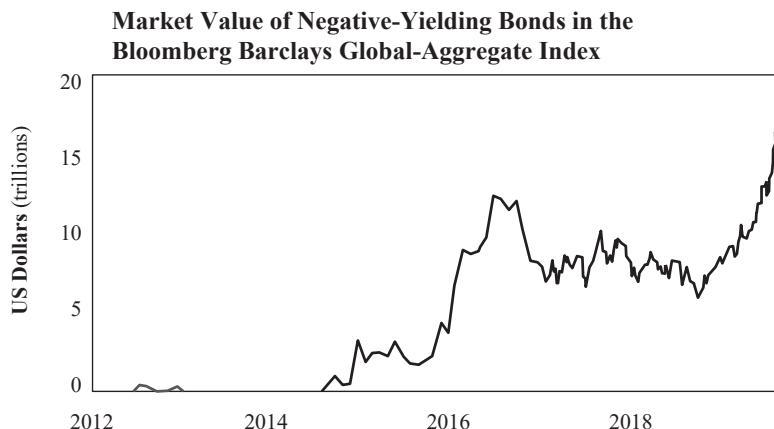
The incentive to save exists, but acquiring savings requires that individuals produce something of value demanded by others. If at first you don't succeed, try, try again. The interests and incentives align perfectly between those holding the currency and those providing goods and services because the script (and relationship) is then flipped after each exchange. Paradoxically, everyone would be incentivized to "save more" in a world in which more money technically could not be saved—the incentive for each individual to produce more is embedded in this system as well. Over time, each person would hold less and less of the currency in nominal terms on average, but each nominal unit would purchase more and more over time (rather than less). The ability to defer consumption or investment and be

rewarded (or simply not be penalized) is the linchpin that aligns all economic incentives.

Bitcoin and the Great Definancialization

The primary incentive to save bitcoin is that it represents an immutable right to own a fixed percentage of all the world's money indefinitely. There is no central bank to arbitrarily increase the supply of the currency and debase savings. By programming a set of rules that no human can alter, bitcoin will be the catalyst that causes the trend toward financialization to reverse course. The extent to which economies all over the world have become financialized is a direct result of misaligned monetary incentives, and bitcoin reintroduces the proper incentives that promote savings. More directly, the devaluation of monetary savings has been the principal driver of financialization, full stop. It should come as no surprise that the reverse set of operations will naturally course correct when the dynamic that created the phenomenon is eliminated.

If monetary debasement induced financialization, it should be logical that a return to a sound monetary standard would have the opposite effect. The tide of financialization is already on its way out, but the groundswell is just beginning to form. And most people do not yet see it coming. For decades, the conventional wisdom has been to invest the vast majority of one's savings. It is a practice that will not reverse overnight. But as the world learns about bitcoin against a backdrop of central banks printing trillions of dollars and anomalies like \$17 trillion in negative-yielding debt, the dots will increasingly be connected.

**FIGURE 5.12**

Source: Bloomberg

“The market value of the Bloomberg Barclays Global Negative Yielding Debt Index rose to \$17.05 trillion [November 2020], the highest level ever recorded and narrowly eclipsing the \$17.04 trillion it reached in August 2019.”

—Bloomberg Markets, November 2020¹⁹

More and more people will begin to question the idea of investing retirement savings in risky financial assets. Negative-yielding debt does not make sense. Central banks creating trillions of dollars in a matter of months doesn't either. All over the world, people are beginning to question the entire construction of the financial system. What if the world didn't have to work this way? What if it was all backward this whole time? And instead of everyone buying stocks, bonds, and layered financial risk with their savings, what if all that was ever really needed was just a better form of money?

Suppose each individual had access to a form of money that was not programmed to lose value. Rather than taking perpetual and open-ended risk, everyone could get back to saving, and the by-product would be greater

19. Cormac Mullen and John Ainger, “World’s Negative-Yield Debt Pile Has Just Hit a New Record,” Bloomberg, 5 November 2020.

economic stability. Simply go through the thought exercise. How rational is it for practically every person to invest in large public companies, bonds, or structured financial products? How much of it is invariably a function of broken monetary incentives? How much of the retirement risk-taking game came about in response to the need to keep up with monetary inflation and the devaluation of the dollar? Financialization was the lead-up to—and the blow-up that caused—the Great Financial Crisis. While not singularly responsible, the incentives of the monetary system caused the economy to become highly financialized. Broken incentives increased the amount of highly leveraged risk-taking and created a broad-based lack of savings, which was a principal source of fragility and instability. Everyone learns the acute difference between money and financial assets in the middle of a liquidity crisis. The same dynamic played out in early 2020 as liquidity crises reemerged.

Fool me once, shame on you. Fool me twice, shame on me. Or so the saying goes. It all traces back to the breakdown of the monetary system and moral hazard introduced to the financial system by misaligned monetary incentives. There is no mistaking it. The instability in the broader economic system is a function of the monetary system. As more of these episodes continue to play out, a growing number of people will continue to seek a more sustainable path forward. With bitcoin increasingly at center stage, there is now a market mechanism that will definancialize and heal the economic system. The process of definancialization will occur as wealth stored in financial assets is converted to bitcoin, specifically as each market participant increasingly chooses to hold a more reliable form of money over risk assets.

Definancialization will principally be observed through growing bitcoin adoption, the appreciation of bitcoin relative to every other asset, and the deleveraging of the financial system. Almost everything will lose purchasing power in bitcoin-denominated terms as bitcoin becomes adopted globally as a monetary standard. Most immediately, bitcoin will gain share from financial assets, which have acted as near-stores of value and monetary substitutes. It is only logical that assets that have long served as monetary

substitutes will increasingly be converted to bitcoin. As part of this process, the financial system will shrink in size relative to the purchasing power of the bitcoin network. The existence of bitcoin as a more sound monetary standard will not only cause a rotation out of existing financial assets. It will also impair demand for future issuances of similar assets and products. Why purchase near-zero-yielding sovereign debt, illiquid corporate bonds, or equity-risk premium when you can own the scarcest asset (and form of money) that has ever existed?

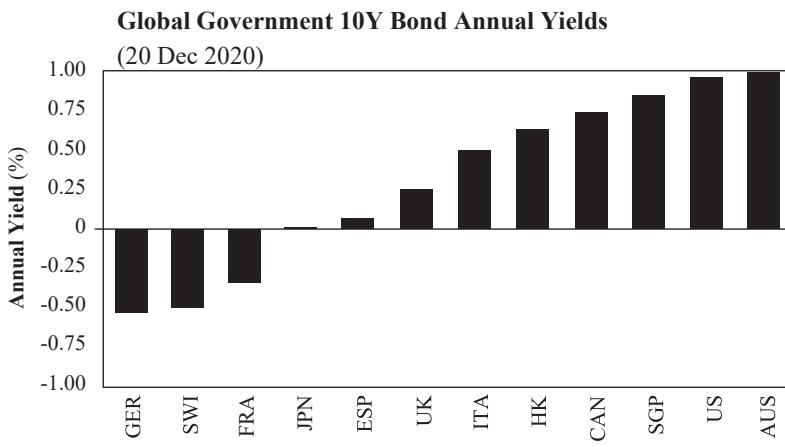


FIGURE 5.13
Source: worldgovernmentbonds.com

The rotation might start with the most obviously mispriced financial assets (e.g., negative-yielding sovereign debt), but everything will ultimately be on the chopping block. Non-bitcoin asset prices will experience downward pressure, creating similar downward pressure on the value of debt instruments supported by those assets. The demand for credit will be impaired broadly, causing the credit system as a whole to contract (or attempt to contract). That in turn will accelerate the need for quantitative easing—an increase in the base money supply—to help sustain and prop up credit markets, which will further accelerate the shift out of financial assets and into

bitcoin. The process of definancialization will feed on itself and accelerate because of the feedback loop between the value of financial assets, the credit system, and quantitative easing.

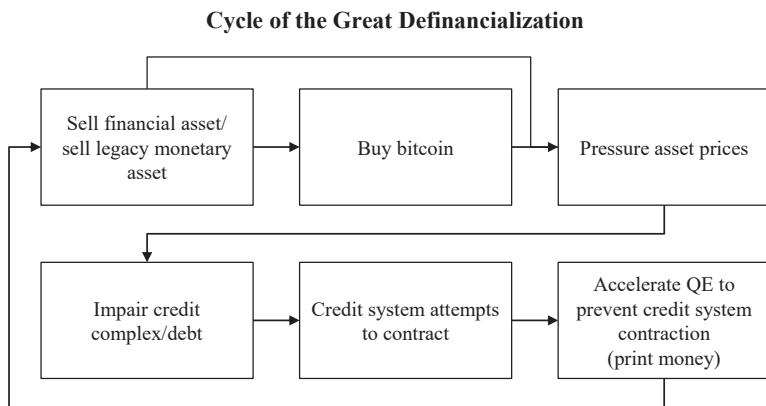


FIGURE 5.14

More substantively, as time passes and as knowledge distributes, individuals will increasingly opt for the simplicity of bitcoin (and its 21 million fixed supply) over the complexity of financial investing and structured financial risk. Financial assets bear operational and counterparty risk, whereas bitcoin is a bearer asset that is perfectly fixed in supply, highly divisible, and easily transferable. The utility of money is fundamentally distinct from that of a financial asset. A financial asset has a claim on the income stream of a productive asset denominated in a particular form of money. The holder of a financial asset is taking risks with the goal of earning more money in the future. Owning and holding money is just that. It is valuable in its ability to be exchanged in the future for goods and services. In short, money can buy groceries. Your favorite stock, bond, or treasury cannot, and there's a reason.

Michael Saylor @michael_saylor

Stocks, Bonds, & Real Estate are all fiat instruments that derive their value from the future stream of cash flows, discounted by the rate of monetary expansion + risk premium. They all fail as a store of value unless they can grow cash flows faster than the Fed can print money.

9 Nov 2020

**FIGURE 5.15**

There is a fundamental difference between savings and investment. Savings are held in the form of monetary assets, while investments are savings that are put at risk. The lines may have been blurred as the economic system financialized, but bitcoin will make the distinction obvious once again. Money with the proper incentive structure will overwhelm demand for complex financial assets and debt instruments. The average person will intuitively and overwhelmingly opt for the security provided by a monetary medium with a fixed supply. Consequently, the balance of power will naturally shift away from Wall Street and back to Main Street.

The banking sector will no longer reside at the epicenter of the economy as a rent-seeking endeavor. Instead, it will sit alongside every other industry and more directly compete for capital. Today, monetary capital is largely captive to the banking system, and that will no longer be true in a bitcoinized world. As part of the transition, the flow of money will increasingly disintermediate from the banking sector. Money will more freely and directly flow among the economic participants who actually contribute value in the real economy.

The function of credit markets, stock markets, and financial intermediation will still exist, but it will all be rightsized. As the financialized economy consumes fewer and fewer resources, and as monetary incentives better align with those that create real economic value, bitcoin will fundamentally restructure the economy. There have been negative societal consequences to disincentivizing savings, but now the ship is headed in the right direction

and toward a brighter future. In the future, gone will be the days of everyone constantly thinking about their stock and bond portfolios, and more time will be spent getting back to the basics of life and the things that really matter.

The difference between saving in bitcoin (not taking risk) and financial investing (taking risk) is night and day. There is something cathartic about saving in a form of money that works in your favor rather than against it. It is akin to having a massive weight lifted off your shoulders that you didn't even know existed. It might not be immediately apparent, but over time, saving in a form of money with proper incentives ultimately allows you to think and worry *less* about money, rather than obsessing over it. Imagine a world in which billions of people, all using a common currency, can focus more on creating value for those around them rather than worrying about making money and financial investing. What that future looks like exactly, no one knows. But bitcoin will definancialize the economy, and it will no doubt be a renaissance.

PART II

Common Misconceptions

CHAPTER SIX

Bitcoin Cannot Be Copied

(Originally published on 2 August 2019)

Alchemy

As kids, we all learn that money doesn't grow on trees. However, despite this timeless wisdom, we have become conditioned at a societal level to believe that it's not only possible but that it's a normal, necessary, and productive function of our economy—specifically the practice of printing massive amounts of money, the modern equivalent of money growing on trees. Ever since the Great Financial Crisis, it has become an uncomfortable fact of life. Before bitcoin, the privilege of creating new money out of thin air was reserved to global central banks, including the Federal Reserve.

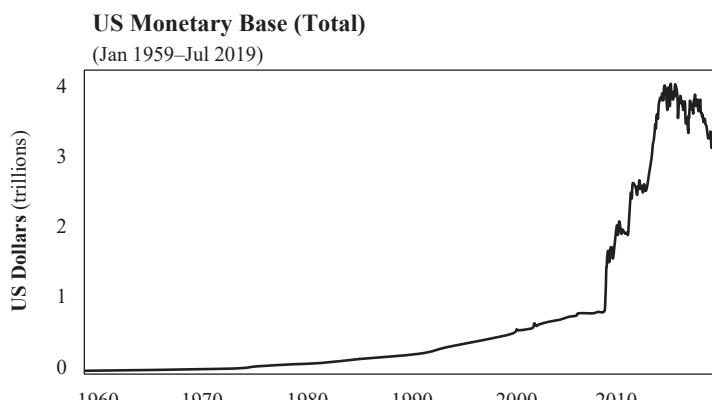


FIGURE 6.1
Source: Federal Reserve Economic Data (FRED)

Bitcoin was specifically created to solve this problem—the problem of printing money. With a fixed supply, bitcoin provides a form of money that everyone can use and one that forever eliminates the ability for anyone to create more units of the currency arbitrarily. However, since the emergence of bitcoin, every Tom, Dick, and Harry seems to think that they too can create money. At a root level, this is the audacity of everyone who attempts to create a copy of bitcoin. Thousands of cryptocurrencies have flooded the scene, each with some promise to improve upon a perceived limitation in bitcoin. Whether by hard-forking out of consensus (Bitcoin Cash), cloning bitcoin (Litecoin), or creating a new protocol with “better” features (Ethereum)—to name a few—each is an attempt to create a new form of money. If bitcoin could do it, why can’t we?

And here we collectively sit—in 2019, as of the time of writing—witnessing the monetization of an economic good (bitcoin) on the free market for the first time since gold emerged as money over thousands of years. Rather than pausing to contemplate the weight of this reality or attempting to understand how or why it is possible, many people skip right past bitcoin and instead focus their attention and efforts on some derivative or some way to solve a problem they didn’t see in the first place. Everyone wants to get rich quick, and so long as there is money, there will also be alchemists. Those who attempt to copy bitcoin are our modern-day alchemists.

Attempts to Copy Bitcoin

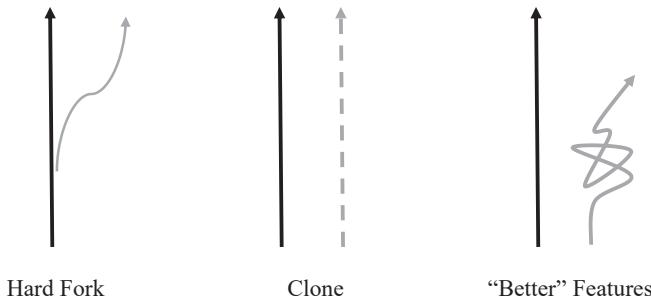


FIGURE 6.2

The alchemists assert that bitcoin is too slow, so they create a “faster” copy. Or that bitcoin lacks the capacity to handle the volume of transactions required to support the global economy, so they create a copy with “greater” scale. Then they declare that bitcoin is too volatile to be a currency, so a “more stable” version is created. It goes on and on. Next, it is that bitcoin is too rigid and needs to be more programmable, so a copy that is “more flexible” is introduced. The alchemists often even tell people that their creation is not money but instead a vehicle for “payments” or a “utility token” or a “global computer fueled by gas.” At the same time, a vision of a world with hundreds, if not thousands, of currencies is sold to unassuming victims. It is all noise, but make no mistake, in each case, it is the alchemist’s attempt to create money.

Bitcoin’s Value Function

If an asset’s primary (if not sole) utility is in its exchange for other goods and services, and if it does not have a claim on the income stream of a productive asset (such as a stock or bond), it must compete as a form of money and will only store value if it possesses credible monetary properties. With each “feature” change, those who attempt to copy bitcoin signal a failure to understand the properties that make bitcoin valuable or viable as money—specifically that bitcoin’s value derives from the fact that the rules are not subject to arbitrary change. When bitcoin’s software code was first released, it was not money. To this day, bitcoin’s software code is not money. You can copy the code tomorrow or create your own variant with a new feature and no one who has adopted bitcoin as money will treat it as such. Bitcoin has become money over time only as the bitcoin network has developed emergent properties that did not exist at inception and that are next to impossible to replicate now that bitcoin exists.

These properties emerged organically and spontaneously as individual economic actors all over the world evaluated bitcoin and decided to store a portion of their wealth in it. As bitcoin’s value increased, it became decentralized. As it became decentralized, it became increasingly difficult to alter the

network's consensus rules or to invalidate or prevent otherwise valid transactions (often referred to as censorship resistance). Notably, it became ever more difficult—if not impossible—to change the rules or incentives that enforce bitcoin's fixed supply. While there remains reasonable debate as to whether bitcoin is sufficiently decentralized or sufficiently censorship-resistant, there are other considerations less subject to debate:

1. Bitcoin represents, by far, the most decentralized and censorship-resistant monetary system in the world today, whether compared to traditional currencies, other digital currencies, or commodity monies like gold.
2. Bitcoin derives its value because it is decentralized and because it is censorship-resistant; it is these properties that secure and reinforce the credibility of bitcoin's fixed supply of 21 million (i.e., why it is an effective store of value).
3. Bitcoin becomes increasingly decentralized and increasingly censorship-resistant as its value increases and as it scales at all levels of the network.
4. Repeat—steps 1-3 create a positive feedback loop.

Emergent Properties of Bitcoin

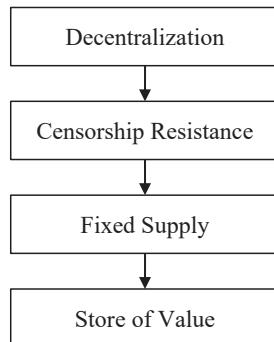


FIGURE 6.3

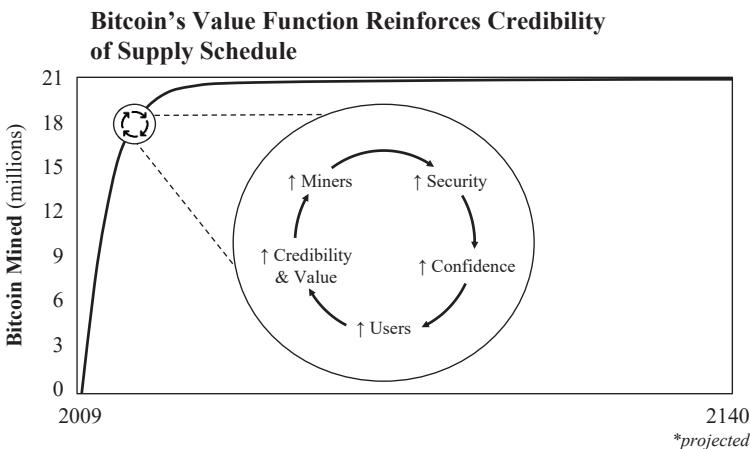


FIGURE 6.4

Economics Systems Converge on One Form of Money

Economic systems converge on a single form of money because the utility of money is liquidity and exchange rather than consumption or production. Every other fiat currency, commodity money, or cryptocurrency is competing for the exact same use case as bitcoin, whether it is understood or not. When evaluating monetary networks, it would be irrational to store value in a smaller, less liquid, and less secure network if a larger, more liquid, and more secure network were accessible. For example, if you worked for two weeks and your employer offered to pay you in a form of currency accepted by one billion people worldwide or a currency accepted by one million people, which would you choose? Would you request 99.9% of one and 0.1% of the other, or would you take your chances with your billion friends? If you are a US resident but travel to Europe one week a year, do you request that your employer pay you 1/52nd in euros each week or take your chances with dollars? The practical reality is that almost all individuals store value in a single form of money, not because others do not exist but rather because it is the most liquid and widely accepted asset to facilitate exchange within their local economy.

Anyone with Venezuelan bolivars or Argentine pesos would opt in to the dollar system if they could. Similarly, anyone choosing to speculate in a copy of bitcoin is making the irrational decision to voluntarily opt in to a less liquid, less secure monetary network. While certain monetary networks are larger and more liquid than bitcoin today (e.g., the dollar, euro, yen), individuals choosing to store a percentage of their wealth in bitcoin are doing so, on average, because of the conclusion that its fixed supply represents a more secure long-term store of value. And, because of the expectation that others (e.g., a billion soon-to-be friends) will come to the same conclusion and also opt in, increasing liquidity and trading partners.

Decentralized → Censorship-Resistant → Fixed Supply → Store of Value

Credible Monetary Properties

Most individuals who create digital currencies neither accept nor admit that what they are creating has to be money to succeed, while those speculating in these assets fail to understand that monetary systems converge on one medium or naively believe that their currency can outcompete bitcoin. None can explain how their digital currency of choice becomes more decentralized and more censorship-resistant, or develops more liquidity than bitcoin. In practice, no other digital currency will likely ever achieve the minimum level of decentralization or censorship resistance required to have a credibly enforced monetary policy.

Bitcoin is valuable not because of a particular feature but because it has achieved finite, digital scarcity, through which it derives its store-of-value property. The credibility of bitcoin's scarcity (and monetary policy) only exists because it is decentralized and censorship-resistant, which in itself has very little to do with software. In aggregate, this drives incremental adoption and liquidity, which reinforces and strengthens the value of the bitcoin network. As part of this process, individuals are simultaneously opting out of inferior monetary networks. This is fundamentally why bitcoin's emergent

properties are next to impossible to replicate, and it is why bitcoin cannot be copied or outcompeted. Bitcoin already exists as an option, and its monetary properties become stronger over time (and with greater scale) at the direct expense of inferior monetary networks.

However, one would likely never come to this conclusion without first developing their own understanding of the following: (1) that bitcoin is finitely scarce; (2) that bitcoin is valuable because it is scarce; and (3) that economic systems converge on one form of money (i.e., one monetary network and system) to facilitate trade. You may come to different conclusions, but this is the appropriate framework to consider when contemplating whether it is possible to copy (or outcompete) bitcoin rather than a framework based on any particular feature set. It is also important to recognize that conclusions drawn by any one person have very little, if any, bearing in the equation. Instead, what matters is what the market consensus believes and what the market converges on as the most credible long-term store of value.

Blockchain Decision Tree

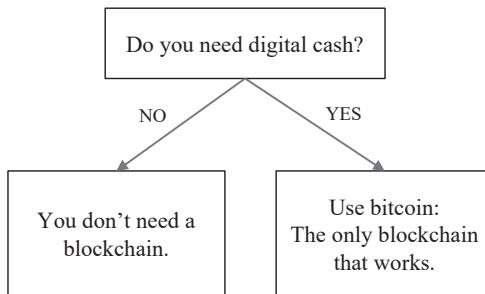


FIGURE 6.5

Source: *The Bitcoin Standard* by Saifedean Ammous

The empirical evidence (price and purchasing power) demonstrates that the market continues to determine that bitcoin is different, despite a significant amount of noise. Before speculating, try to understand why bitcoin works and why it is unique. When someone inevitably tells you about a “better” bitcoin or some differentiating feature, remember that the market,

which has come to this same crossroad many times over the last decade before you, has considered those trade-offs and chosen bitcoin over the rest of the field for very rational reasons.

The Minority Rule

Nassim Taleb writes about how a very small intransigent minority can force its preference on the majority, referring to this phenomenon as “the minority rule” and explaining why “The Most Intolerant Wins.”²⁰ Monetary systems are a perfect example of this phenomenon. If a very small minority converges on the conclusion that bitcoin has superior monetary properties and will not accept another form of currency as money, while market participants with less conviction accept both bitcoin and other currencies, the intolerant minority wins. This is exactly what is happening in the global competition for digital currency supremacy. A small minority of market participants have determined that only bitcoin is viable, while at the same time rejecting the monetary properties of all other digital currencies. Because of its intransigence, the minority slowly forces its preference on the majority.

The Minority Rule

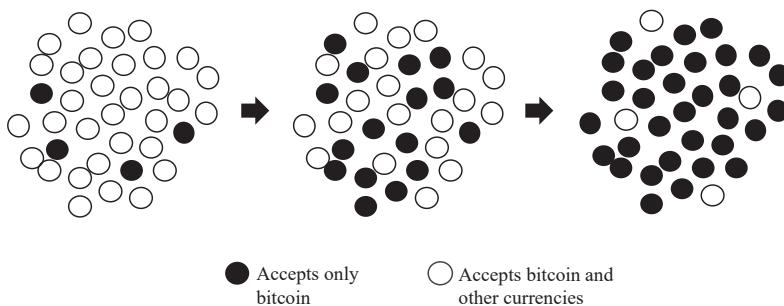


FIGURE 6.6

20. Nassim N. Taleb, “The Most Intolerant Wins: The Dictatorship of the Small Minority,” *Incerto* (blog), Medium, 19 August 2016.

In the world of digital currencies, diversifying by picking the field is the equivalent of letting the crowd choose what your future money will be while resigning yourself to only a fraction of what you otherwise would have saved. Evaluate the trade-offs, anchor yourself in the fundamentals, and consider the minority rule before trading your hard-earned value for a perceived get-rich-quick flyer that you do not understand. Money doesn't grow on trees.

“Bitcoin is a remarkable cryptographic achievement, and the ability to create something that is not duplicable in the digital world has enormous value.”

—Eric Schmidt,
former CEO and executive chairman, Google²¹

21. Eric Schmidt and Jared Cohen, “The New Digital Age: Authors Eric Schmidt and Jared Cohen in Conversation with Facebook’s Sheryl Sandberg,” interview by Sheryl Sandberg (Mountain View, CA: Computer History Museum, 3 March 2014), catalog number 102740112.

CHAPTER SEVEN

Bitcoin Is Not Too Volatile

(Originally published on 9 August 2019)

A Common Refrain

Has someone you respect ever told you that bitcoin doesn't make sense and could never be money because it is volatile? The idea that something as volatile as bitcoin could be money seems entirely inconsistent. You may have agreed after witnessing the price of bitcoin rise exponentially only to subsequently crash. Perhaps you wrote it off, assuming bitcoin was dead since it was no longer in the public spotlight. But then a few years pass, and you wake up to find that bitcoin hasn't died, and somehow, its value is even greater. Finally, you start to think maybe you were wrong.

The list of bitcoin skeptics is long and distinguished,²² but the noise and natural skepticism also contribute directly to the antifragile nature of bitcoin. People who store wealth in bitcoin are forced to think through first principles to understand the characteristics of bitcoin that otherwise seem to contradict an establishment view of money, which ultimately hardens their understanding and conviction. Bitcoin volatility is one of these oft-criticized characteristics. A common refrain among skeptics, especially central bankers, is that bitcoin is too volatile to be a store of value, medium of exchange, or unit of account. Given its volatility, why would anyone use bitcoin as a savings

22. "The Skeptics: A Tribute to Bold Assertions," Satoshi Nakamoto Institute, accessed 8 August 2019.

mechanism? And how could bitcoin be effective as a transactional currency for payments if its value could suddenly drop tomorrow?

The principal use case for bitcoin today is not as a payments rail but instead as a store of value, and those storing wealth in bitcoin are typically not doing so for merely a day, a week, or even a year. Bitcoin is a long-term savings mechanism, and stability in the value of bitcoin will emerge over time as a function of mass adoption. In the interim, volatility is the natural result of price discovery as bitcoin advances down the path of its monetization event and toward full adoption. Separately, bitcoin does not exist in a vacuum. Most individuals or businesses are not singularly exposed to bitcoin, and exposure to multiple assets, as in any portfolio, mutes the volatility of any single asset.

Not Volatile ≠ Store of Value

Volatility and an asset's ability to store of value are often misunderstood as being mutually exclusive. If an asset is volatile, it does not mean that asset will be an ineffective store of value. The opposite is also true. If an asset is not volatile, it will not necessarily be an effective store of value. The dollar is a prime example. The dollar is not volatile (today, at least), and it is a poor store of value.

“Volatile things are not necessarily risky, and the reverse is also true.”

—Nassim Taleb²³

The Fed has been highly effective in slowly devaluing the dollar, but always remember: *gradually, then suddenly*. Many people experience this critical mental block when thinking about bitcoin as a currency, and it is largely a function of time horizon. When central bankers across the world point to bitcoin as a poor store of value and not being functional as a currency due to volatility, they are thinking in days, weeks, months, and quarters while the rest of us plan for the long term: years, decades, and generations.

23. Nassim N. Taleb, *Skin in the Game: Hidden Asymmetries in Daily Life*, (Random House, 2018).

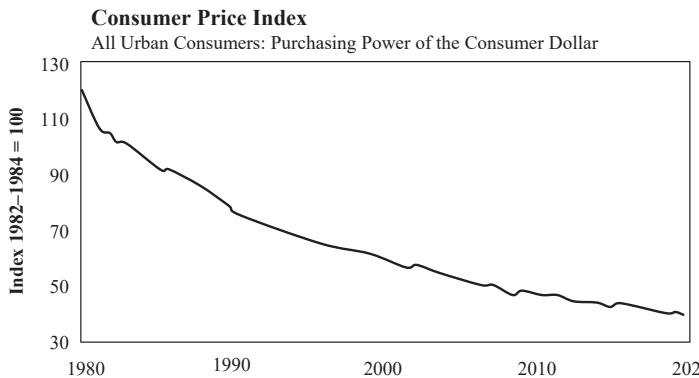


FIGURE 7.1
Source: US Bureau of Labor Statistics

Despite the logical explanations, volatility is one aspect of bitcoin that particularly confounds the experts. For example, Bank of England Governor Mark Carney recently commented that bitcoin “has pretty much failed thus far on [...] the traditional aspects of money. It is not a store of value because it is all over the map. Nobody uses it as a medium of exchange.”²⁴ The European Central Bank (ECB) has mused on Twitter that bitcoin is “not a currency,” noting that it is “very volatile” while at the same time reassuring everyone that the ECB can “create” money to buy assets—the very same function that causes the euro to persistently loses purchasing power.

The lack of self-awareness is not lost on anyone here, but Mark Carney and the ECB are not alone. From former Fed Chairs Ben Bernanke²⁵ and Janet Yellen²⁶ to current US Treasury Secretary Mnuchin²⁷ and US President Trump²⁸—all have at times trumpeted the idea that bitcoin is flawed as a currency or as a store of value due to its volatility. None seem to fully appreciate,

24. David Milliken, “BoE’s Carney says Bitcoin has pretty much failed as currency,” *Reuters*, 19 February 2018.

25. Ben Bernanke, “Ben Bernanke on Bubbles, Bitcoin, and Why He’s Not a Republican Anymore,” interview by Matt Phillips, *Quartz*, 19 November 2015.

26. Janet Yellen, speech, Canada Fintech Forum, 29 October 2018, Montreal, Canada.

27. “White House Press Briefing by Treasury Secretary Steven Mnuchin on Regulatory Issues Associated with Cryptocurrency,” news release, US Department of the Treasury, 15 July 2019.

28. Billy Bambrrough, “Donald Trump Unleashes Sudden Attack on Bitcoin,” *Forbes*, 12 July 2019.

or at least admit, that bitcoin is a direct response to the systemic problem of governments creating money via central banks or that bitcoin volatility is a necessary and healthy function of price discovery. Luckily, bitcoin is not too volatile to be a currency, and often the “experts” are not experts at all. The empirical evidence shows that bitcoin has proven to be an exceptional store of value over any extended time horizon despite its volatility. So how could an asset such as bitcoin be both highly volatile and an effective store of value?

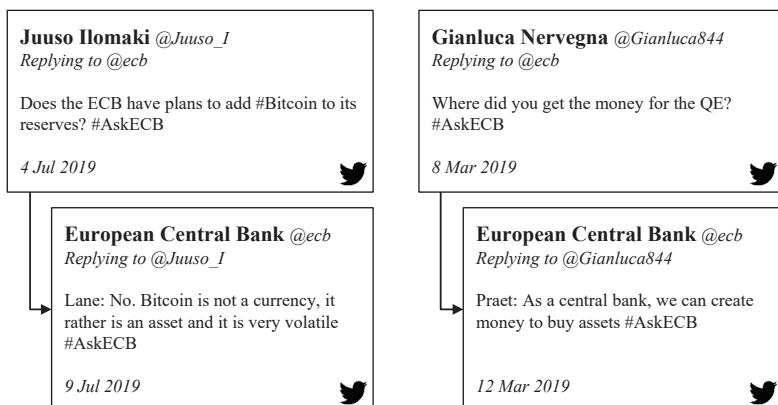


FIGURE 7.2



FIGURE 7.3

Source: Bitstamp

Bitcoin Value Function Revisited

Consider why there is fundamental demand for bitcoin and why bitcoin is naturally volatile. Bitcoin is valuable because it has a fixed supply, and it is volatile for the very same reason. The fundamental demand driver for bitcoin as money is its scarcity. To revisit bitcoin's value function, decentralization and censorship resistance reinforce the credibility of bitcoin's scarcity (and fixed supply schedule) which is the basis of bitcoin's store-of-value use case.

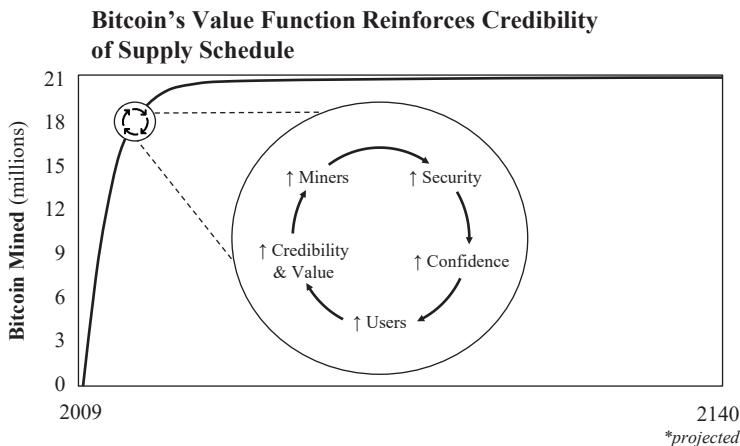


FIGURE 7.4

While demand is increasing by orders of magnitude, there is no supply response because bitcoin's supply schedule is fixed. The disparity in the rate of increase in demand (variable) versus supply (fixed) combined with imperfect knowledge among market participants causes volatility as a consequence of price discovery. In "The Black Swan of Cairo," Nassim Taleb writes, "Variation is information. When there is no variation, there is no information."²⁹ As bitcoin's value increases, it communicates information despite its volatility. In fact, volatility itself is information. The variation is the information. A higher

29. Nassim N. Taleb and Mark Blyth, "The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous," *Foreign Affairs* 90, no. 3 (May/June 2011), 6.

value (dependent on variation) causes bitcoin to become relevant to new pools of capital and new entrants, which then stokes a wave of adoption.

Adoption Waves and Volatility

Distribution of knowledge and development of infrastructure fuel adoption waves and vice versa. It is a virtuous feedback loop and a function of both time and value. As bitcoin's value rises, it captures the attention and mind-share of a much wider audience of potential adopters, who then begin to learn about the fundamentals of bitcoin. Similarly, an appreciating asset base attracts additional capital, not only to use bitcoin as a store of wealth but also to build incremental infrastructure (e.g., more on-ramps and off-ramps, custody solutions, payments layers, hardware, mining, etc.). Developing an understanding of bitcoin is a slow process, as is building infrastructure. However, both fuel adoption, which further distributes knowledge and justifies building more infrastructure.

*Knowledge → Infrastructure → Adoption →
Value → Knowledge → Infrastructure*

Fixed Supply vs. Expanding Demand

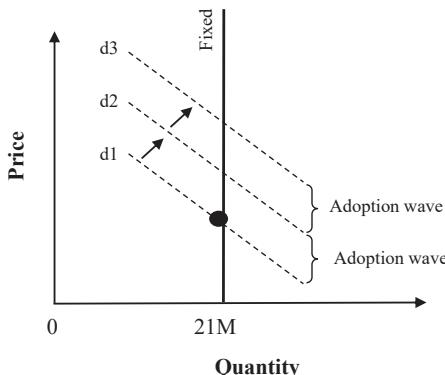


FIGURE 7.5

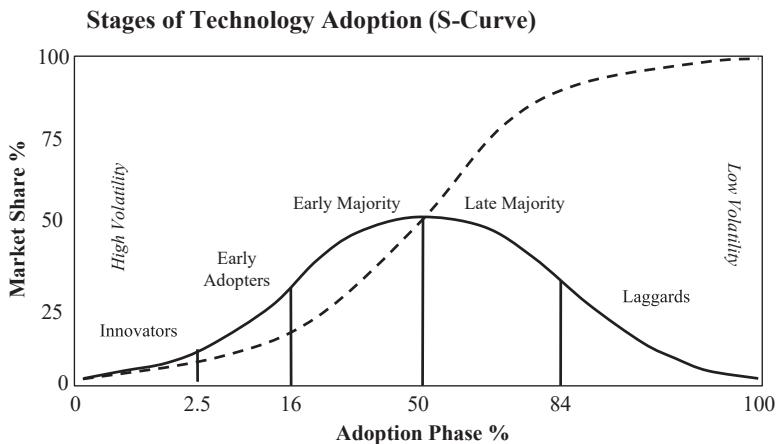


FIGURE 7.6

Source: *Diffusion of Innovations* by Everett M. Rogers (1962)

Today, bitcoin is still nascent, and current adoption likely represents <1% of terminal adoption. As a billion people adopt bitcoin, new adoption will represent an increase by orders of magnitude relative to the embedded base of demand for any foreseeable future period, which is the fundamental source of volatility—high variable demand relative to a lower stable base. However, with each new adoption wave, the value of bitcoin will also reset higher because of higher base demand. Bitcoin volatility will only decline as the holder base reaches maturity and as the rate of new adoption stabilizes. Said another way, when one billion people are using bitcoin, adoption will have increased by 20x, but the next billion adopters would only represent an increase of 50%. All while the supply of bitcoin remains on a fixed schedule.

So long as increases in adoption represent orders of magnitude, volatility is unavoidable. But on the path to full adoption, volatility will naturally and gradually decline, and practically only when incremental adoption begins to represent a fraction of embedded base demand.

“Establishment economists deride the fact that bitcoin is volatile, as if you can go from something that didn’t exist to a stable form of money overnight. It’s completely ludicrous.”

—Vijay Boyapati³⁰

At present, what happens between adoption waves is the natural function of price discovery as the market converges on a new equilibrium, which is never static. In bitcoin hype cycles, the rise, fall, stabilization, and rise again are almost rhythmic. It is also naturally explained by speculative fear, followed by the accumulation of fundamental knowledge and the addition of incremental infrastructure. Rome wasn’t built in a day, and neither is bitcoin. Volatility and price discovery are core to the process of bitcoin adoption.

Bitcoin Adoption Waves (Simplified)

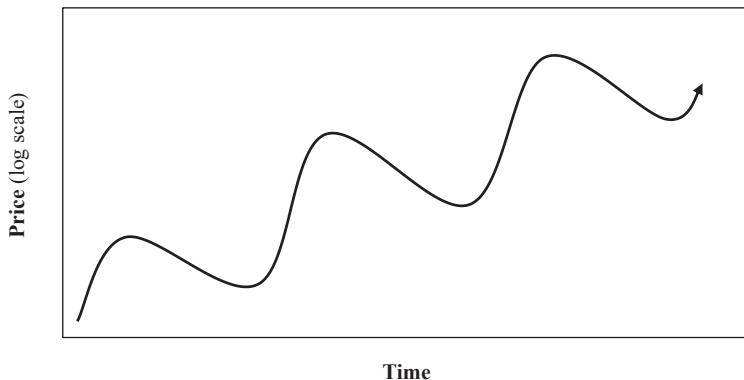


FIGURE 7.7

30. Vijay Boyapati, “How Bitcoin Mentally Captures People,” interview by Stephen Livera, *Stephen Livera Podcast* (ep. 2), 28 July 2018.

Historical Adoption Wave

For a more tangible explanation of the relationship between volatility and value, it is helpful to think about the most recent wave of adoption (as of the time of writing), a four-year period between mid-2015 and mid-2019.

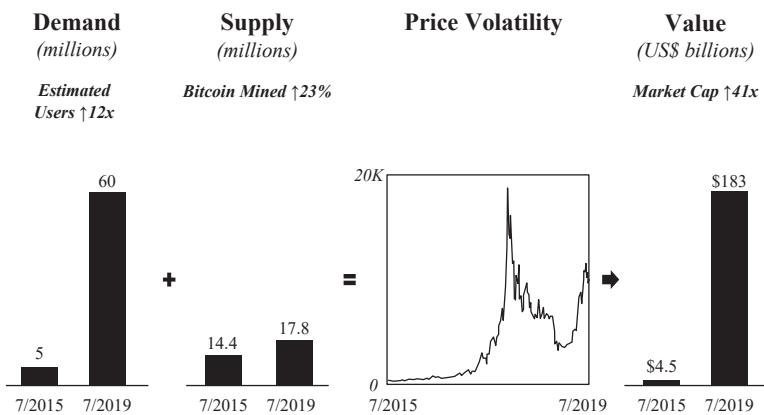


FIGURE 7.8

While adoption can never be fully quantified due to the decentralized and pseudonymous nature of the network, for illustrative purposes, let's assume adoption increased by ten times over a four-year period (Coinbase users increased 13x, from 2.3 million to 30 million, between mid-2015 and mid-2019).³¹ Yet, over the same period, the supply of bitcoin only increased by approximately 23%. As a massive adoption wave occurred, it was met by bitcoin's fixed supply schedule. What would one expect when demand increases by an order of magnitude, but supply only increases by 23%? And what would happen if the knowledge and capital of the new entrants naturally vary a great deal? Recognize that every first-time bitcoin buyer is pricing it for the first time. So in a hypothetical scenario of adoption increasing by ten times, nine out of every ten market participants are necessarily pricing bitcoin for the first time.

31. Coinbase User Data, compiled by Alistair Milne, Altana Digital Currency Fund, 2019.

The very logical end result is higher volatility and a higher terminal value if even a small percentage of new entrants convert to long-term holders (which is exactly what happened). New adopters who initially purchased bitcoin as a speculative investment during its astronomical rise slowly accumulate knowledge and convert to long-term holders. This stabilizes base demand at a far higher terminal value compared to the prior adoption cycle. Because bitcoin is nascent, the aggregate wealth stored in it is still very small on a relative basis ($\sim \$200$ billion). Hence, the rate of change between marginal buyers and sellers (price discovery) represents a significant percentage of the base demand, resulting in volatility. As base demand increases, the rate of change will come to represent a smaller and smaller percentage of the base, reducing volatility over time and likely only after several more adoption cycles.

Managing Volatility

If someone can accept that bitcoin volatility is both natural and unavoidable, the question becomes why does bitcoin adoption continue to grow despite the volatility? Turned around, why does volatility not prevent the adoption of bitcoin as a monetary standard? Very simply: diversification, portfolio allocation, time horizon, and knowledge distribution. A global network (bitcoin) exists through which you can store value in a currency with a fixed supply and transfer value over a communication channel to anyone in the world, and it is currently valued at less than \$200 billion (as of the time of writing) because very few people understand it. Today, Facebook alone is worth more than \$500 billion, and US household assets are estimated to be valued at \$125 trillion.³²

Bitcoin volatility would be an issue if it existed in a vacuum. However, it does not. Diversification comes in the form of real productive assets as well

32. Board of Governors of the Federal Reserve System, *Z.1 Financial Accounts of the United States: Flow of Funds, balance Sheets, and Integrated Macroeconomic Accounts, First Quarter 2019*, Federal Reserve Statistical Release, 6 June 2019, 138.

as other monetary and financial assets, which mutes the impact of bitcoin's present volatility. Separately, information asymmetry exists. Those who understand bitcoin also understand that, in time, the cavalry is coming. More people will adopt bitcoin for the reason that it has fixed supply, but only as knowledge distributes. These concepts are obvious to those with exposure to bitcoin who actively account for its volatility in short- and long-term planning. But it is less obvious to the skeptics, who struggle to grasp that bitcoin adoption is not an all-or-nothing proposition.

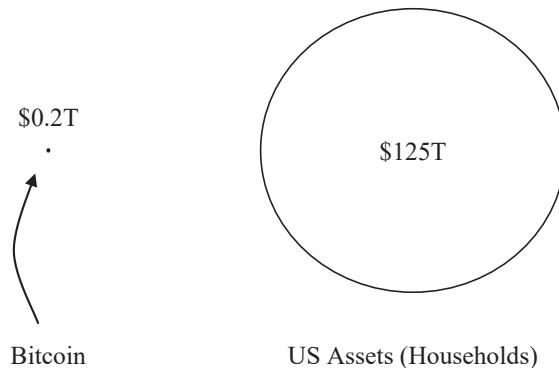


FIGURE 7.9

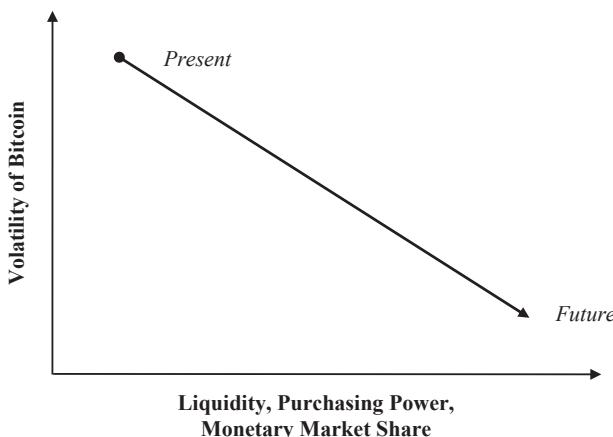


FIGURE 7.10

Bitcoin will continue to steal market share in the global store of value competition because of its superior monetary properties. But the function of an economy is to accumulate capital that improves quality of life, not money. Money is merely the economic good that enables the coordination required to accumulate that capital through trade. As a fundamentally better form of money, bitcoin will gain purchasing power relative to inferior monetary assets (and money substitutes), despite being less functional as a transactional currency today in direct trade. As it does, bitcoin will reduce the need for, but not eliminate, stocks, bonds, real estate, and other real assets as stores of value. During its monetization, these assets will continue to represent sources of diversification that mute the impact of bitcoin's day-to-day volatility.

The example below highlights the risk and return profile of a portfolio with 1% and 3% exposure to bitcoin, compared to a traditional 60% equity, 40% bond portfolio.³³ It provides a look into how all volatility is typically managed and how a very small allocation to bitcoin historically would have resulted in greater return, with the volatility of bitcoin muted by exposure to other assets in a diversified portfolio.

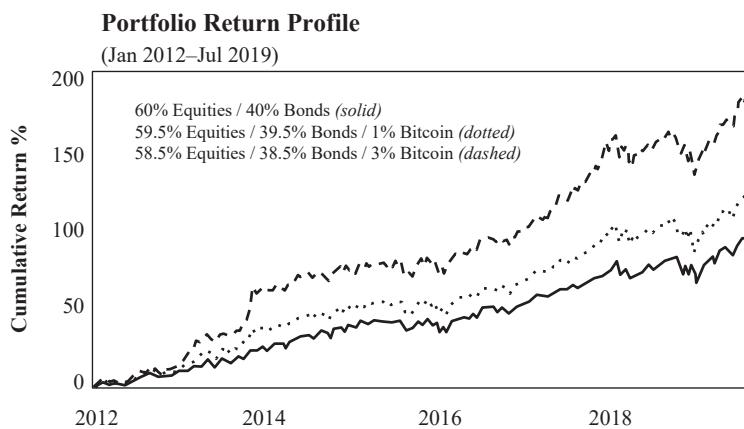


FIGURE 7.11

Source: "The Investment Case for Bitcoin," VanEck, 2019

33. "The Investment Case for Bitcoin," VanEck, 21 October 2019.

“It would be irresponsible to have an exposure to Bitcoin that one cannot afford to lose because the risk of losing the principal is very real. But it would be almost as irresponsible to not have any exposure at all.”

—Wences Casares³⁴

While failure is a *possibility* and significant drawdowns are inevitable, each day that bitcoin does not fail, its survival becomes more and more likely.³⁵ And over time, as bitcoin’s value and liquidity increase due to its superior monetary properties, its purchasing power will also increase in terms of real goods and services. As its purchasing power represents a larger and larger share of the economy, its volatility relative to other assets will inevitably and proportionally decrease.

The End Game

Bitcoin will become a transactional currency over time. In the interim, it would be far more logical to spend a depreciating asset (dollars, euros, yen, or gold) and save in an appreciating asset (bitcoin). On bitcoin’s path to full monetization, its use as a store of value must come as a logical first step, and bitcoin has proven to be an incredible store of value despite its volatility. As adoption matures, volatility will naturally fall, and bitcoin will increasingly become a medium of direct exchange.

Consider the individual or business that demands bitcoin in direct exchange for goods and services. Logically, that individual or business would first need to have determined that bitcoin would hold its value over a particular time horizon. If one did not believe in the fundamental demand case for bitcoin as a store of value, they simply would not trade real-world goods and services in return. Bitcoin will transition to a transactional currency only as

34. Wences Casares, “The Case for a Small Allocation to Bitcoin,” Kana and Katana, 1 March 2019.

35. This dynamic is known as the Lindy Effect. For more information, see “Lindy Effect,” Wikipedia.

more people first understand why it will store value. As that occurs, bitcoin's liquidity will gradually migrate from other monetary assets (dollar, euro, yen, etc.) to the direct exchange for real goods and services. It will not be a flash cutover or a binary process. On a more standard path, adoption fuels infrastructure, and infrastructure fuels adoption. Transactional infrastructure is already being built, and more material investment will be prioritized as a sufficient number of individuals first adopt bitcoin as a store of wealth, necessitating the need for bitcoin payments.

Bitcoin's Path to Full Monetization

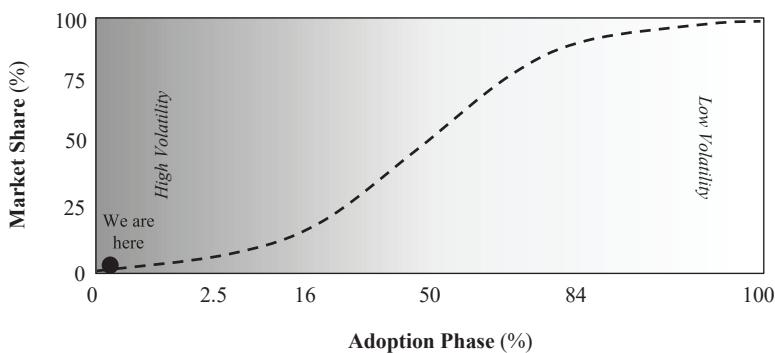


FIGURE 7.12

Bitcoin's day-to-day liquidity will scale and diversify as a function of both, reducing volatility over time, but unavoidably, bitcoin's fixed supply and rapid growth in adoption will continue to result in near-term volatility. Stability will emerge organically as bitcoin is adopted by the entire world. It is the literal opposite model of that pursued by the Bank of England, the European Central Bank (and its Twitter account), the US Federal Reserve, and the Bank of Japan. Central banks *manage* currencies to mute short-term volatility, creating instability that leads to long-term volatility. Volatility in bitcoin is the natural function of monetary adoption, and it ultimately strengthens the resilience of the bitcoin network by eliminating market imbalances, driving long-term stability. Variation is information.

“Complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks. This is one of life’s packages: there is no freedom without noise—and no stability without volatility.”

—Nassim N. Taleb and Mark Blyth³⁶

“The Federal Reserve is not currently forecasting a recession.”

—Ben Bernanke,
former chair, Board of Governors, US Federal Reserve³⁷

36. Nassim N. Taleb and Mark Blyth, “The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous,” *Foreign Affairs* 90, no. 3 (May/June 2011), 6.

37. Ben Bernanke, “Financial Markets, the Economic Outlook, and Monetary Policy,” remarks before Women in Housing and Finance and Exchequer Club, Washington, DC, Speech, 10 January 2008.

CHAPTER EIGHT

Bitcoin Does Not Waste Energy

(Originally published 16 August 2019)

The Long Game

When you board a commercial flight, you always hear the same safety briefing just before takeoff. You may even know it by heart. Every time, without fail, flight attendants instruct passengers to put on their oxygen masks before tending to any children should the cabin lose air pressure. Instinctively, it's counterintuitive. Logically, it makes all the sense in the world. Make sure you can breathe first so that the child dependent on you can breathe too. The same principle applies to the coordination function of money in an economy and the resources required to protect that function. In a more philosophical safety briefing, the flight attendant might say:

Please make sure the money supply is secure so that we can continue to coordinate the economic activity of millions of people to build these incredibly complex planes that afford you the opportunity to even contemplate the problem I'm about to explain.

We will come back to this, but you can never hope to understand the justification for the amount of energy bitcoin consumes without first appreciating the fundamental role money plays in coordinating economic activity. What is money? How does it work? How should it work? What is its function in society? If you haven't stopped to ask these questions, you can't begin to grasp the weight of the problem bitcoin intends to solve. And

without an appreciation for the problem, the cost to secure the solution will never seem justified.

Concerned onlookers raise a red flag about the amount of energy consumed by the bitcoin network, without the necessary baseline. The concern stems from the idea that the energy consumed by the bitcoin network could otherwise be utilized for more productive functions or that it is detrimental to the environment. Both fail to appreciate just how critical bitcoin's energy consumption is. In the long run, there may be no more critical use of energy than that which is deployed to secure the integrity of a monetary network—in this case, the bitcoin network. However, that doesn't stop those ignorant of the problem from raising concerns.

“The fundamentally wasteful nature of bitcoin mining means there’s no easy technological solution coming.”

—*The Guardian*³⁸

“In the context of climate change, raging wildfires, and record-breaking hurricanes, it’s worth asking ourselves hard questions about Bitcoin’s environmental impact.”

—*Vice Media*³⁹

Bitcoin Energy Consumption

Bitcoin is secured by a decentralized network of nodes (computers running the bitcoin protocol). Economic nodes within the network generate, validate, and relay transactions, as well as validate and relay bitcoin blocks (time-sequenced groups of transactions). Mining nodes perform similar functions while also performing bitcoin's proof-of-work function to generate, solve, and transmit blocks to the rest of the network. By carrying out

38. Alex Hern, “Bitcoin’s Energy Usage Is Huge—We Can’t Afford to Ignore It,” *The Guardian*, 17 January 2018.

39. Christopher Malmo, “One Bitcoin Transaction Consumes as Much Energy As Your House Uses in a Week,” *Vice Media*, 1 November 2017.

this work, miners validate the network's transaction history and provide a clearing function for current transactions, which all other nodes then check for validity. Think of the clearing function of the New York Fed but on a completely decentralized basis every ten minutes (on average).

The work performed (running cryptographic hashing functions) requires computer processing power contributed by miners, operating twenty-four hours a day, seven days a week. This processing power requires energy. For context, at 75 exahashes (75,000,000,000,000,000,000 hashes) per second,⁴⁰ the bitcoin network currently consumes approximately 7 gigawatts (7,000,000,000 watts) of power, which translates to ~\$9 million in energy per day (~\$3.3 billion per year), assuming an average cost of 5 cents per kilowatt-hour (kWh) for illustrative purposes. Based on US national averages, the bitcoin network consumes as much power as approximately 6 million homes.⁴¹ By no means is this insignificant, but it is also what secures the bitcoin network.

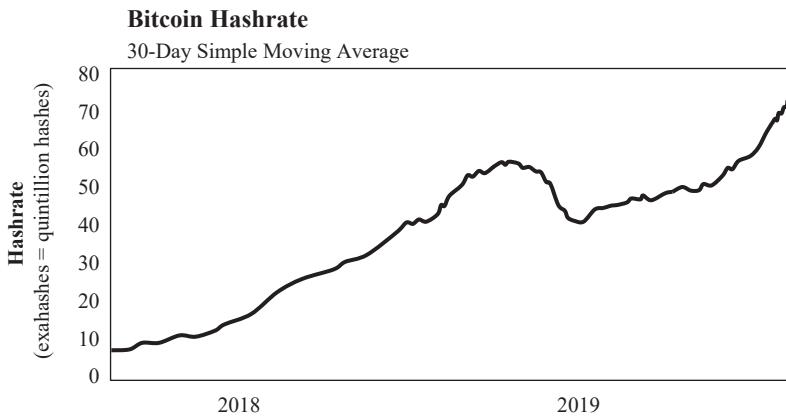


FIGURE 8.1
Source: bitinfocharts.com

40. BitInfoCharts, "Bitcoin Hashrate historical chart," September 2017–August 2019, accessed 15 August 2019.

41. "2015 RECS Survey Data," Residential Energy Consumption Survey, US Energy Information Administration.

How could this much energy usage be justified? And how much energy will bitcoin consume when a billion people are using it? The dollar works just fine, right? Well, that's just the thing. It doesn't. These resources are being devoted to fix a problem most don't understand exists, which makes justifying a derivative cost challenging. People who do not understand why bitcoin has fundamental value are functionally incapable of doing a cost-benefit analysis. Without having any grasp of the benefit side of the equation, it is definitionally impossible. But to help ease the pain of environmentalists and social justice warriors, bitcoin advocates often point out several countervailing narratives to make it seem more palatable:

- Bitcoin will spur innovation in the development of renewable-energy technology and resources.
- Bitcoin consumes energy that would normally go to waste, including natural gas that is flared or vented into the atmosphere.
- Bitcoin consumes only the energy that the free market will bear at a free-market rate.
- Bitcoin consumes stranded energy resources that would otherwise not be economical to develop for domestic or industrial use.
- The nature of bitcoin energy demand will improve the efficiency of energy grids.

These considerations help enumerate why a simple view that bitcoin's energy consumption is necessarily wasteful or necessarily bad for the environment fails the proverbial test. However, one could never justify the marginal cost without first appreciating the enormity of the monetary problem bitcoin intends to solve. Bitcoin represents a solution to the systemic issues within our legacy monetary framework, and it relies on energy consumption to function. Economic stability depends on the function of money, and bitcoin provides a sound monetary framework that the legacy system is missing, which is why there is no more important long-term use of energy than securing the bitcoin network. So rather than expand on the

many individual counterpoints to the mainstream narrative, there is no better place to focus than the first-principle problem: the money problem or the global QE (quantitative easing) problem.

The Function of Money

The problems stemming from our current monetary system are enormous, though most people fail to recognize them. Most experience the symptoms of the problem in their daily lives (working harder for longer, accumulating debt, and still barely getting by) but cannot identify the root cause. To identify a solution, one must first see and understand the problem. The problem that exists is with our money, and the negative impact it has on society is pervasive.

Money is the good that facilitates economic coordination between parties who otherwise would not have a basis to cooperate. It is the good that allows society to function and to accumulate the capital that improves our standard of living—recognizing that capital takes different forms for different people. While some people say money is the root of all evil, Hayek more appropriately describes it as an instrument of freedom:

“Money is one of the greatest instruments of freedom ever invented by man. [...] If we strive for money, it is because money offers us the widest choice in enjoying the fruits of our efforts.”

—Frederich A. Hayek⁴²

More specifically, money is the good that allows for specialization and the division of labor. It enables individuals to pursue their own interests. It is how individuals communicate their preferences to the world, whether through work or leisure, and it is what creates the range of choice we all take for granted. Our modern economy is built on the foundation of freedom that money provides—enabling a highly complex and specialized system, which affords a standard of living that prior generations would find hard to imagine.

42. Friedrich A. Hayek, *The Road to Serfdom*, condensed version (*Reader's Digest*, April 1945).

To simplify the concept, Milton Friedman (expanding on Leonard Read's 1958 essay⁴³) explains the complexity of producing a standard lead pencil. He details how no individual alone is capable of producing and assembling all the necessary resources. The wood, the saw to cut the wood, the steel to make the saw, the iron ore to make the steel, the lead, the rubber for the eraser, the brass ring, the yellow paint, and the glue, etc. Friedman explains how making a single pencil requires the coordination and cooperation of thousands of people, including people who don't speak the same language, who likely practice different religions, and who may even despise each other if they were ever to meet in person.⁴⁴

If that is just the pencil, now consider the complexity of our modern economy, from cars to airplanes to the internet, and even to your local grocery store. Modern supply chains are so complex and so specialized that they require the coordination of millions of people to deliver any of these basic functions. The orchestration of all the activity that fuels global trade is only made possible through the function of money.

A Living Example: Venezuela

Venezuela provides a tangible macro and micro example of money's vital role in economic coordination and the dysfunction that follows when it fails. Despite being one of the most oil-rich countries in the world, Venezuela's currency has recently hyperinflated as an end-game function of monetary debasement. As its currency has deteriorated, basic economic functions have broken down to the point where getting food at grocery stores or critical healthcare is no longer a given. It's a full-blown humanitarian crisis, and at the root level, it's a function of Venezuela no longer possessing a stable currency to coordinate economic activity and facilitate production of the goods the country needs to trade.

43. Leonard E. Read, "I, Pencil: My Family Tree as Told to Leonard E. Read," *The Freeman* (December 1958).

44. Milton Friedman, "The Power of the Market," *Free to Choose*, volume 1, PBS, 1980. The lesson of the pencil begins at 15:40.

How does this relate to bitcoin and energy consumption? As an energy-rich country, oil was (and is) Venezuela's primary export, or rather, the principal good it needs to produce in order to trade. Despite its vast energy resources, Venezuela's oil production has plummeted.⁴⁵

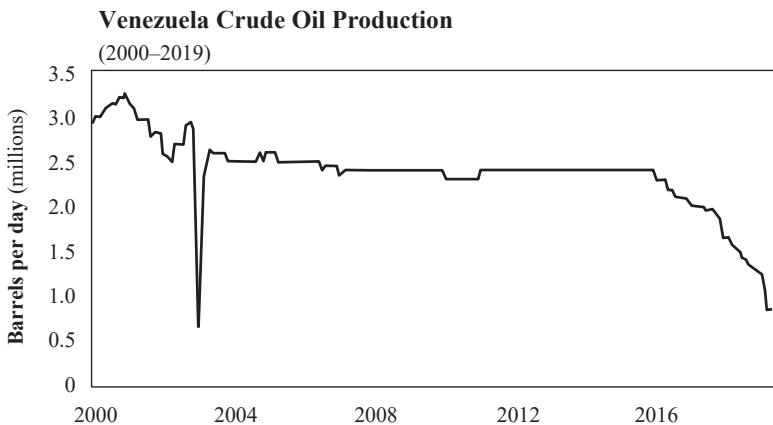


FIGURE 8.2
Source: US Energy Information Administration

Venezuela can no longer import the technology or coordinate the resources it needs to extract its primary trading currency—oil. This has caused significant deterioration in its local economy, impairing its ability to produce the electricity needed to power its energy grids, causing extended blackouts, and preventing the delivery of essential services such as power, clean water, or healthcare.

The situation in Venezuela is devastating, and it is a function of the economic deterioration caused by hyperinflation. Monetary debasement distorts the price mechanism of a currency, which creates and sustains economic imbalances. As economic coordination deteriorates, complex supply chains become disrupted, resulting in a decline in the supply of real goods (e.g., food on shelves, oil production, power, etc.) and an imbalance between supply and

⁴⁵ Emily Sandys, “Venezuelan Crude Oil Production Falls to Lowest Level Since January 2003,” Today in Energy, US Energy Information Administration, 20 May 2019.

demand. As more money is created, real goods become scarce relative to the supply of money, which causes the very function of money to break down. Individuals are incentivized to trade out of local currency as quickly as possible as basic goods become more and more scarce, creating a “run” on basic necessities and causing the currency to hyperinflate. This is Economic Deterioration by Monetary Manipulation 101.

The Developed-World Application

Many sitting comfortably in the developed world will look at Venezuela and think *it could never happen here*, but this ignores first principles. Whether or not it is well understood, the market structure of the Venezuelan bolivar or the Argentine peso is identical to that of the dollar, the euro, and the yen. The Fed may be better at managing stability (for now), but it does not change the fact that the underpinnings of all fiat currency systems are the same. The cost to print or digitally create a US dollar is the same as the cost to create a Venezuelan bolivar—zero. The cost to produce a trillion dollars-worth of either currency is also zero, and the long-term consequence to the viability of the currency is the same.

As historical context, the US Federal Reserve expanded the monetary base from \$190 billion in 1984 to \$840 billion at the beginning of 2008, an increase of \$650 billion over twenty-four years. Then, in response to the 2008 financial crisis, the Fed increased the money supply by nearly \$3.6 trillion over the subsequent five years to a peak of \$4.2 trillion in 2014.⁴⁶ The debasement occurred gradually until the financial crisis, which then resulted in a far more drastic increase in the money supply. In aggregate, the base money supply has increased by 22x since 1984. And it is not without consequence. As a function of quantitative easing, the US economy now sits further out on the same fragile ledge that existed during the financial crisis in 2008.

46. Federal Reserve Bank of St. Louis, “Adjusted Monetary Base (DISCONTINUED),” retrieved from Federal Reserve Economic Data (FRED), Federal Reserve Bank of St. Louis, July 2019.

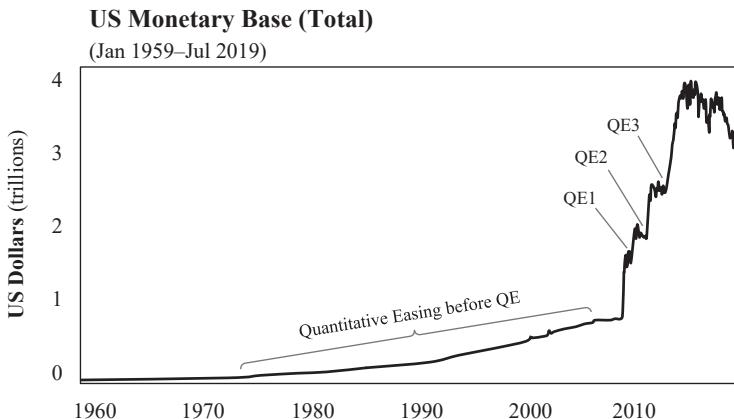


FIGURE 8.3
Source: Federal Reserve Economic Data (FRED)

If you believe the developed world is not in a precarious situation or does not rely on a monetary foundation similar to Venezuela's, I would respectfully point to the Fed and its historical track record. Blink faith placed in this institution lacks all common sense. Consider the following quote from a resident Fed economist during the aftermath of the 2008 financial crisis, at a time when the Fed was in the middle innings of creating \$3.6 trillion new dollars as part of quantitative easing:

“I want to just emphasize that I think the gaps in our understanding of the interactions between the financial sector and the real sector are profound.”

—David Wilcox, August 2011
Associate Economist, US Federal Reserve⁴⁷

An honest review of history demonstrates the ill-suited temperament of those put in charge of managing central banks. While admitting profound gaps in their ability to understand the implications of actions taken on the

⁴⁷. *Minutes of the Federal Open Market Committee*, a joint meeting of the Federal Open Market Committee and the Board of Governors of the Federal Reserve System, Washington, DC, 9 August 2011.

real economy, the response was to continue down the same path, printing even more money and expecting a different result—with no credible reason as to why. The printing of money causes the currency to deteriorate over time until it ultimately fails completely. Now, as the world faces the consequences of the response to the last crisis, individuals have a choice between two great contrasts: a centrally managed currency designed to lose its value or a decentralized currency with a fixed supply. The latter comes with a cost in the form of energy consumption, but the positive externality will be long-term economic stability provided by a form of money that cannot be printed.

Economic Stability via Energy Consumption

Future economic stability is why there can be no fundamentally more important source of energy demand than the security of bitcoin's monetary system, especially as central banks print more and more money. If you wait to see the obvious signs of hyperinflation, you will have waited too long. But Venezuela is not just an example of what transpires due to hyperinflation. It is a living example of the importance of energy production to the functioning of society. Some energy input is required to produce everything we consume in our daily lives. The coordination of those energy inputs is dependent on the reliability and stability of the money we use.

Ignore your morning coffee for a minute and think about the basics: clean water, sanitation, food, gasoline, electricity, medicine, basic healthcare, etc. The coordination of resources to deliver these services is dependent on a functioning form of money. When a monetary system breaks down, social coordination and even the social fabric of society begin to go with it. If the basis of all trade is energy, and if money is necessary to coordinate trade, the highest and best use of that energy should first be to protect the monetary system. Put your proverbial oxygen mask on first and then shift to dependents. Secure the money—the foundation of trade—and then focus on all of the derivatives.

Any concerns about the amount of energy bitcoin consumes or will consume is a red herring. It is not that electricity that could otherwise power

homes should be sacrificed. Instead, it is that the electricity to power those homes will no longer be produced if a reliable form of money does not exist to coordinate economic activity and facilitate trade—just as what happened in Venezuela. In practice, bitcoin will not compete for energy resources that fuel our economy's basic productive and consumptive functions in a zero-sum way. Instead, bitcoin's function as a currency system will ensure that those very energy needs can continue to be fulfilled.

What would be regrettable for society is if more countries were to deteriorate into Venezuela-style economic and humanitarian disasters, where basic health and human services could not be reliably provided. The goal here is not to present a dystopian vision of the future but to articulate the importance and interconnectedness of the functions of money and energy in complex, highly specialized economies.

“If it prevents even one more tragic incidence of hyperinflation, the energy consumption required to mine [bitcoin] will be the best bargain humanity ever got.”

—Saifedean Ammous⁴⁸

Bitcoin represents a backup switch to legacy currencies that are failing, and it is soon to be the primary engine powering both local and global trade. Setting aside the systemic risks that currently plague the US and global financial systems, bitcoin is a fundamentally more sound monetary system from the ground up, secured by the production and consumption of energy. You do not have to believe that the dollar's fate will be that of the Venezuelan bolivar to recognize the importance and interplay between the stability of money and the production of energy resources. The risk inherent in even the possibility of hyperinflation is so negatively asymmetric that the price of bitcoin's energy consumption is of small relative cost.

Bitcoin will consume any and all energy resources necessary to secure its monetary network, which is inherently driven by the base demand to

48. Saifedean Ammous, “The Problem Bitcoin Solves,” *The Spectator*, 10 November 2018.

hold it as a currency. Every ounce of energy bitcoin uses is devoted to securing its fixed supply and clearing transactions for final settlement. There is no waste. The more people that value the long-term stability bitcoin provides, the more energy the network will consume in total. In the end, this consumption will ensure all other derivatives of energy consumption will continue to be fulfilled, which is why there is no more important long-term use of energy than securing the bitcoin network. Put a price on economic stability and the economic freedom a stable monetary system provides. That is the true justification for the amount of energy bitcoin should and will consume. Everything else is a distraction.

CHAPTER NINE

Bitcoin Is Not Too Slow

(Originally published on 23 August 2019)

The Ultimate Technology Leap

In the book *Zero to One*, Peter Thiel outlines the impact of new technologies in building a non-zero-sum future.⁴⁹ From the advent of the steam engine to the shift from typewriters to computer processors, he presents several examples of individuals and companies who have introduced innovations that resulted in step-function changes. Thiel distinguishes between true step-function innovation as being *0 to 1*—innovation that creates something entirely new—and the scaling or incremental improvement of such innovation as being *I to n*.

However, Thiel also expressed the view that innovation has largely stagnated since the early 1970s, with technological progress being primarily *I to n* rather than *0 to 1*, which may have been true until the advent of bitcoin. As a monetary system, bitcoin is the ultimate *0 to 1* technology leap, and it is fundamentally differentiated from the class of step-function innovation that is the book’s focus. Bitcoin is a monetary protocol built on digital scarcity, the impact of which will be far more consequential than steam engines and computer processors because of the critical role money plays in coordinating virtually all other economic resources.

49. Peter Thiel and Blake Masters, *Zero to One: Notes on Startups, or How to Build the Future* (Crown, 2014).

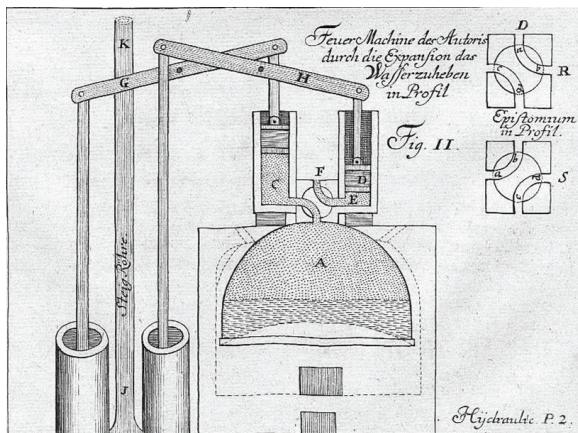


FIGURE 9.1
 "Steam Engine" by Jacob Leupold
(Theatri Machinarum Hydraulicarum II, 1725)

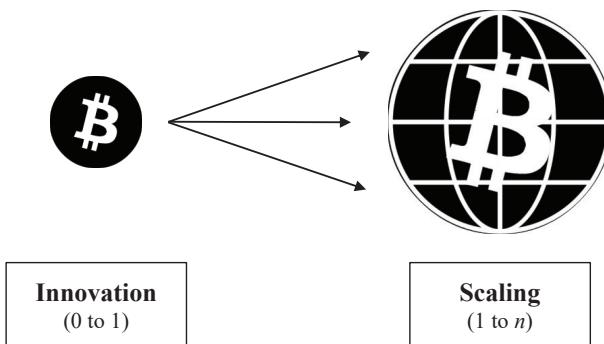


FIGURE 9.2

A Step-Function Change

There's a new meme floating around the internet; whatever the problem, *bitcoin fixes this*. Negative yielding debt? Bitcoin fixes this. Endless global war? Bitcoin fixes this. Cancel culture? Bitcoin fixes this. Financial crises? Bitcoin fixes this. We're not exactly sure how just yet, but it is an articulation of the balancing effect a sound and stable monetary system will have on every aspect

of society. As the coordination function of society, money allows people to cooperate who otherwise would not have a basis to do so via trade. Bitcoin represents a form of money that cannot be printed, which solves a problem for practically every living being on earth. It is global, permissionless, and resistant to all forms of censorship, which makes it functionally accessible to anyone and everyone. The collective benefit that follows may not literally cure every ill in the world. But the invention of a step-function change monetary network is fundamentally different from any single product or company because money is the economic good that coordinates and makes possible the production of all other economic goods. Bitcoin is *0 to 1*, and the solutions to scale bitcoin (from 1 to *n*) will naturally be incremental.

“The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore how to dispense with the need of conscious control and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do.”

—Friedrich A. Hayek⁵⁰

Hayek writes about the invention of money and the price mechanism as the tool that allows society to dispense with the need for “conscious control.” Bitcoin is the superior successor to this mechanism, and its *0 to 1* innovation is finite scarcity, not payments or transaction speed. While bitcoin’s property of scarcity still needs further stress testing, it is a profound achievement, and it is what makes bitcoin unique. Never before has any form of money, let alone a digital one, been finitely scarce. The significance (and relevance) is that finite scarcity serves as the foundation for the hardest form of money that has ever existed—hardest in the sense that, in a terminal state, no one can produce any more or at all—and anyone in the world can use it. There will only ever be 21 million bitcoin. That is the *0 to 1* achievement and a phenomenon that almost certainly will not be repeated (see “Bitcoin Cannot Be Copied”).

50. Friedrich A. Hayek, “The Use of Knowledge in Society,” *American Economic Review* 35, no. 4 (September 1945): 527.

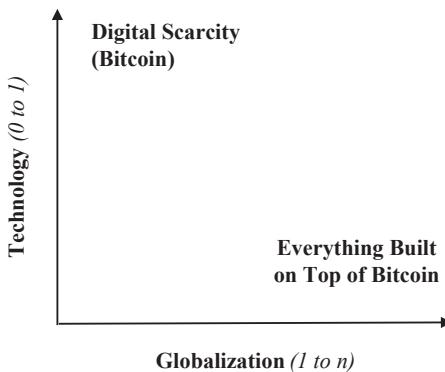


FIGURE 9.3
Inspired by *Zero to One* by Peter Thiel (2014)

Every other problem that bitcoin will have to overcome is more pedestrian relative to scarcity. Digital payments? The idea that human ingenuity could create finite digital scarcity but could not then layer on payments technology to scale does not logically follow. Payments technology is just one of the many *1 to n* innovations that will be built on top of bitcoin to globalize its adoption. Not only are payments an easier problem to solve, but they are not a critical path that needs solving *today*—as of the time of writing. The primary use case for bitcoin today is as a savings mechanism. Over time, as adoption increases and more infrastructure is built, bitcoin will evolve into a transactional currency facilitating direct commerce, but that process will occur on a gradual basis. In most cases, an individual or business would reasonably need to first understand why bitcoin will store value into the future as a savings mechanism before accepting bitcoin as a form of payment in direct commerce or trade. It's a logical progression. And as the shift occurs, bitcoin adopters will continue to leverage legacy monetary systems and payment rails in parallel until a time when the world is fully on a bitcoin standard.

Not a Payment Rail

As traditionally defined, a payment rail is a network or platform that acts as financial plumbing, moving money from payer to payee in return for goods or services. The bitcoin blockchain will likely never be a layer for mass payments, but there is considerable debate on this topic. Many believe that for bitcoin to be “successful,” it needs to be a one-stop shop, combining the roles of currency issuer, settlement layer (confirming transactions), and payment rail. While bitcoin fulfills the first two functions beautifully (currency issuer + settlement layer), it is categorically not a payment rail as traditionally defined. For reasons of speed and scale but most importantly due to the nature of payments, bitcoin fails the *payment rail* test. The good news? The bitcoin network does not need to be a payment rail—in the Visa sense—to function perfectly well as money and solve a massive problem.

Much of the confusion in the philosophical (rather than technical) debate stems from the opening salvo of the bitcoin whitepaper: “a Peer-to-Peer Electronic Cash System.”⁵¹ It does say “purely peer-to-peer” after all. But this has been interpreted by some to imply that bitcoin needs to be able to handle every last transaction in the world between any two peers. Separately, others contend that if bitcoin transactions cannot occur at the scale or speed of Visa or Mastercard, the network is structurally flawed. Essentially, the argument made by skeptics is that if bitcoin cannot meet both of these standards, it fails on its promise. Thankfully, it does not. Visa and Mastercard are not money themselves. Each is a credit system that settles the transfer of money between two parties. It is also not practical or sensible for every person on earth to retain records of every transaction by and between every other person, which is what functionally occurs for each individual or business running a bitcoin node maintaining records of all bitcoin transactions throughout history.

51. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (whitepaper, 31 October 2008).

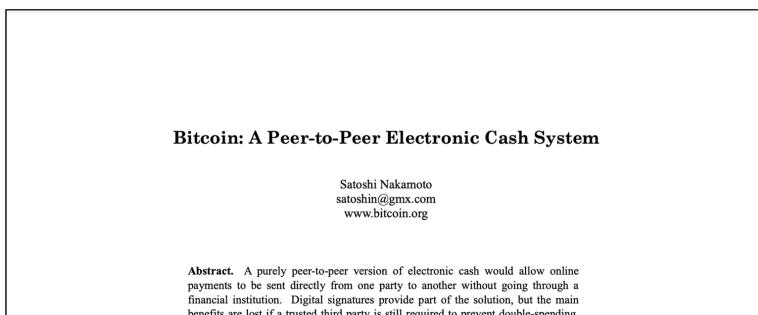


FIGURE 9.4

For additional background, valid bitcoin transactions are confirmed in timestamped batches and included in a “block.” Blocks are solved every ten minutes *on average* (but not precisely). The next block may be solved in one minute or twenty minutes, thirty seconds or thirty-six minutes. The network adjusts such that blocks are solved *on average* every ten minutes. How could a merchant or transaction processor operate in a world this slow or this unpredictable? Separately, each bitcoin transaction includes data, and each block has a defined maximum (or limited) amount of data it can include, typically defined as block space, to be accepted as valid. While the bitcoin network does not have a fixed transaction capacity by count, each bitcoin transaction consumes a certain amount of block space, which limits capacity. As a function of limited space and capacity, blocks include approximately 2,700 transactions on average. With ten-minute average block intervals, six blocks per hour, twenty-four hours per day, 365 days per year, that equates to a network transaction capacity of approximately 145 million transactions per year, equivalent to approximately 4.6 transactions per second. Visa, on the other hand, processes 124 billion transactions per year at a rate of ~4,000 transactions per second.⁵²

52. Visa Inc., *Form 10-K: Annual Report*, United States Securities and Exchange Commission (SEC) archives, fiscal year ended 30 September 2018.

Block Height	Timestamp	Transaction Count	Size (KB)	Weight (KWU)
591274	8/22/2019 3:11:33 PM (CDT)	2705	1336.157	3992.754
591273	8/22/2019 2:52:28 PM (CDT)	2434	1185.475	3992.651
591272	8/22/2019 2:46:54 PM (CDT)	2206	1202.922	3992.806

FIGURE 9.5
Source: blockstream.info

How can bitcoin be the purely peer-to-peer engine that powers the global financial system if it operates at nearly one one-thousandth the scale and speed of Visa alone? It is a false dilemma. The reality has always been that if bitcoin were to have a non-zero value, the consequence would be a system so valuable to so many people that any base layer would not be able to handle all transactions without sacrificing decentralization or censorship resistance. Each of which is fundamental to bitcoin credibly enforcing its fixed supply. Without these properties, bitcoin would not be a *0 to 1* innovation, and its value function would break down entirely.

Ultimately, the bitcoin protocol layer provides the function of currency issuance and final settlement. It is not capable of storing every small purchase, including your Starbucks coffee, for the rest of time for everyone, nor is that necessary for bitcoin to function as money. If it were the case, all transactions by all people, no matter how big or how small, would have to be validated and stored by every other person on earth. Without a mechanism to align the interests of network participants, a “tragedy of the commons” problem would exist. The result would be a less secure currency system subject to centralization. Instead, bitcoin has a mechanism to limit transaction throughput at the base layer, prioritizing security and decentralization, while necessarily shifting aspects of bitcoin’s peer-to-peer transactional architecture to separate layers that interoperate with bitcoin. These trade-offs

have been made very intentionally in order to secure the foundation of bitcoin's monetary system.

Decentralization → Censorship Resistance → Fixed Supply

The scarcity of the currency (i.e., the fixed supply) is tied to the scarcity of block space and derivatively, transaction capacity. The latter preserves and promotes decentralization in importantly distinct ways and aligns incentives throughout the bitcoin network at each a security, transactional, and node level. But more importantly, everything critical in bitcoin is enforced by a consensus of network participants, including its fixed supply and the space within each bitcoin block, which limits the number of transactions it can process. This is the fundamental difference between bitcoin and the legacy financial system: monetary policy by consensus rather than by central bank. Bitcoin's creator and early contributors collectively produced a system that ultimately removed critical decisions from any central authority, instead deferring to the wisdom of market consensus. It is a system that is flexible enough to be adapted but rigid enough that any material change is exceptionally difficult. As a consequence, network peers have to decide, on a decentralized basis, how best to scale bitcoin. Through this consensus mechanism, bitcoin dispenses with the need for "conscious control."

Security Trade-Offs

Everything comes with trade-offs, but there are two holy grails in bitcoin: enforcing a fixed supply and preventing individual units of the currency from being spent multiple times (the double-spending problem). The value of bitcoin is derived from its ability to secure each of these functions on a decentralized, trustless basis, and both are inextricably linked to the bitcoin network's limited transaction capacity. Think of the space within each bitcoin block as valuable digital real estate. All market participants seeking to clear bitcoin transactions have to compete for block space. Scarcity in block

space is the function by which bitcoin's shared resource is optimized and how bitcoin solves for the “tragedy of the commons” problem. Competition for this scarce resource ensures that it is used efficiently and that its value is maximized. Scarcity causes market participants to compete with each other, bidding up the value of block space rather than shifting negative externalities onto the rest of the network.

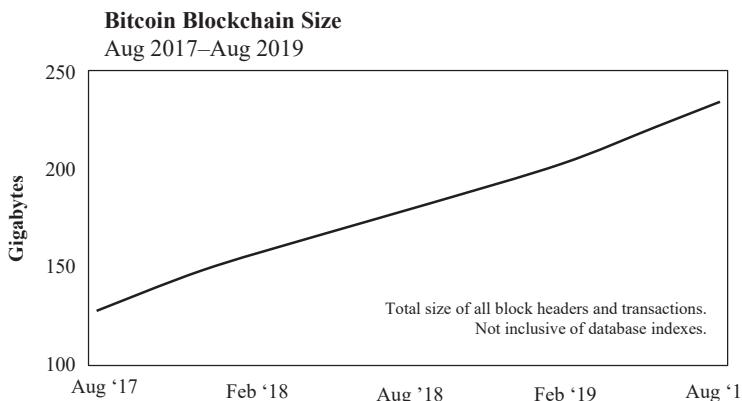


FIGURE 9.6

Source: blockchain.com

In bitcoin's free market, the highest-value and most profitable transactions are prioritized. Without scarcity in block space, this market mechanism would break down. It is less important that bitcoin optimizes for transaction capacity and more critical that scarcity in block space exists. No one really knows the optimal amount of transaction capacity at any point in time, partly because demand is ever-changing but also because it generally grows over time. The critical piece is that block space is both known and scarce, which enables market participants to plan and, ultimately, compete. The commons are never depleted. Instead, innovation is spurred to figure out how best to utilize a scarce resource (e.g., improving transaction efficiency and moving lower-value transactions to new payment layers). Scarcity of block space also has the effect of creating a predictable and limited rate of growth in the overall size of bitcoin's blockchain, which directly correlates to

the cost and complexity of running a bitcoin node, protecting and promoting decentralization as a derivative but intentional consequence.

As discussed in “Bitcoin Does Not Waste Energy,” miners secure the bitcoin network by devoting real-world energy resources to run cryptographic hashing functions in an attempt to solve bitcoin blocks. By solving blocks, miners validate history and clear current transactions, which are then checked, validated, and propagated by the rest of the network nodes. In return for devoting resources to perform this function and secure the network, miners get paid in the network’s native currency (bitcoin). The actual compensation paid to miners comes in two forms: newly issued bitcoin and transaction fees. Miners have to reliably expect that aggregate compensation will hold its value into the future in order to devote resources today.

Era	Block Height (Start–End)	Coinbase Reward	Inflation Rate (Era Total)	Bitcoin Issued (Era)	Cumulative Bitcoin Issued (End of Era)
1	0–209,999	50	–	10,500,000	10,500,000
2	210,000–419,999	25	50%	5,250,000	15,750,000
3	420,000–629,999	12.5	16.67%	2,625,000	18,375,000
4	630,000–839,999	6.25	7.14%	1,312,500	19,687,500
5	840,000–1,049,999	3.125	3.33%	656,250	20,343,750
<i>cont.</i>					

FIGURE 9.7

Approximately every four years, the amount of newly issued bitcoin paid to miners is cut in half (referred to as the bitcoin “halving” or “halvening”). Today, with each block, 12.5 new bitcoin are issued. When the next halving event occurs in approximately May 2020 (as of the time of writing), that amount will be reduced to 6.25 new bitcoin per block. And approximately four years after that, 3.125 new bitcoin per block will be issued. This process will continue until the smallest unit of bitcoin

($1/100,000,000^{\text{th}}$) is reached—after which, no new bitcoin will be issued. It is this issuance function that governs bitcoin’s fixed supply of 21 million. It also shifts compensation to secure the network from (mostly) new bitcoin today to a system relying entirely on transaction fees paid by users of the network to bitcoin miners in the future.

How does this relate to transaction capacity? If it were not for the scarcity of capacity in each bitcoin block, there would not be a mechanism to create a transaction-fee market. Scarcity in block space limits transaction capacity and creates competition between market participants to clear transactions, in turn causing users to bid up the value of that space (i.e., digital real estate), while also incentivizing efficient use because it comes with cost. Without a transaction-fee market, the only mechanism to pay miners to secure the network would be to alter bitcoin’s fixed monetary policy and perpetually increase supply. But recall that bitcoin’s fixed supply (21 million) is the basis of its store-of-value property, which is where the rubber meets the road. By creating scarcity in block space, the network also ensures the integrity of bitcoin’s fixed supply, which makes the whole value function work. Hence, scarcity is a far more important property than either the speed or ultimate capacity of transaction throughput.

*Fixed Block Space → Limited Transaction Capacity
→ Fee Market → Fixed Supply of Bitcoin*

The real problem bitcoin is intending to solve is that of money and the endless printing of money, not “payments” as the term is loosely and commonly used. Accordingly, there is nothing more important than securing the money supply and its long-term integrity, especially not transaction throughput to support everyday payments. It’s not a chicken-and-egg problem either. Security necessarily comes first. In short, the future of bitcoin is far more secure in a world where all market participants can depend on it having a reliably fixed and scarce supply while accepting lower transaction throughput or speed today as trade-offs. What good are high transaction

throughput and faster speeds if the fundamental value of the underlying currency is at risk? The existing financial system has already made the opposite trade-off—high transaction throughput and fast transactions by way of centralization but with the cost of an architecture susceptible to systemic monetary debasement. Bitcoin represents the alternative, and it would not be rational to make the same mistake twice. But luckily, it is not an either-or dilemma. Rather, it is one of logical order. Prioritize security first, and then allow the market to innovate to scale transaction capacity in a way that does not sacrifice security.

Bitcoin ≠ Visa

Ultimately, bitcoin is not competing with Visa for supremacy in global payments. Instead, bitcoin is competing with the dollar, euro, yen, and gold as money. Any comparison to Visa, its transaction volume, or its transaction speed is fundamentally flawed. Bitcoin fulfills the role of currency issuer and final settlement. As a result, the proper comparison would be between bitcoin and the Federal Reserve as both a currency issuer and clearinghouse of dollars. No one makes the mistake of confusing the functions of Visa for that of the New York Fed, but for some reason, the comparison is often made between Visa and bitcoin.

While it would require time and investment, Visa's payment network could sit on top of the bitcoin network much as it sits on top of the existing banking system. Rather than clearing dollars through a central bank, the final settlement of transactions would clear in bitcoin through the bitcoin network. In the existing architecture, the payment layer (Visa) and the settlement layer (banking network/central bank) are separate and distinct. Visa helps move dollars, but Visa is not the dollar. Visa is a technology company that provides a service. It has 17,000 employees.⁵³ Bitcoin has none.

53. Visa Inc., *Form 10-K*.

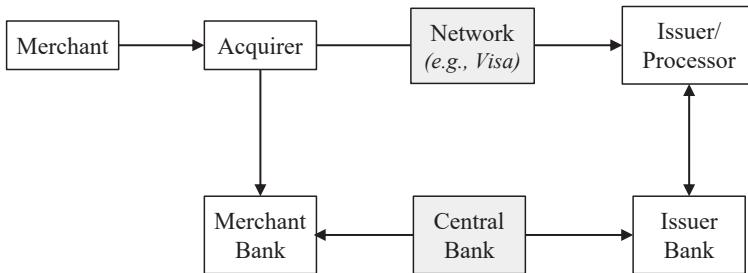


FIGURE 9.8

Consumers generally associate swiping a Visa card (or the equivalent) at a point-of-sale terminal with instantaneous payment, but this is not the case. Whether using credit or debit, Visa is an inherently trust-based credit system. Balances must first be checked, transactions are then authorized, and only then may settlement occur. Dollars are not actually cleared through a central bank or settled at the point of sale *every* time a transaction is processed either. Individual transactions are also never really cleared. Instead, transactions are batched, netted, and settled at a later point in time. Only then are accounts credited with proper balances. So when someone attempts to equate a Visa transaction at point of sale with final settlement, that is simply not the way the world works. But that is the comparison implicitly being made when someone attempts to compare Visa with bitcoin.

Bitcoin vs. the Federal Reserve

When compared to its real competition (the dollar, euro, yen, etc., and the Fed, ECB, BoJ, etc.), bitcoin begins to look like a Ferrari—final global settlement approximately every ten minutes, twenty-four hours per day, seven days a week, 365 days a year on a permissionless basis. Compare this to the existing permissioned financial system, which is subject to multiple layers of bank and central bank intermediaries and only open during “business” hours. This is the great misnomer that exists within bitcoin. Those who

believe bitcoin is too slow or lacking in transaction capacity are comparing it to the wrong application. A network of banks *could* be set up on top of the bitcoin network, and the payments system could function as it does today.

The pushback on this as a method to scale bitcoin is the risk of centralization. If bitcoin were to just sit in banks, it would increase the possibility that the bitcoin network could be co-opted and undermined by a network of banks and central banks, whether to force changes to network consensus rules or censor end users. The point is that it would be functionally *possible* and that money and payments technology are distinct problems. The fundamental reason is that there are two sides to every value transfer. One side almost always involves money, and the other is the fulfillment of goods and services. The nature of trade is such that the two sides of a value transfer generally occur through different processes and at different points in time.

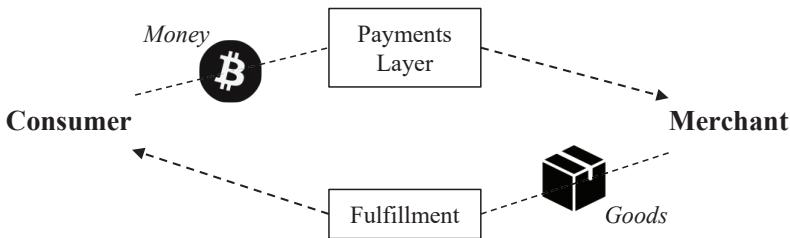


FIGURE 9.9

Think about the settlement of currency on one side and the transfer of title to a home on the other. Or perhaps, payment for a good on Amazon and the fulfillment of that good two days later. Two different processes inevitably occurring at two different times. It is also important to recognize that bitcoin has no knowledge of the outside world, whether the identities of the parties involved or the second leg of a value transfer. All bitcoin knows is how to issue and validate currency (whether a bitcoin is genuinely and validly a bitcoin). This is really the function and limitation of any base currency system. Payments layers provide a bridge to a problem with two-sided risk,

between currency settlement and the fulfillment of goods and services. Gold solved mass payments via bank centralization, the dollar, the Fed, and large payments processors such as Visa. Bitcoin likely solves payments through a technologically superior mechanism, but more to the point, solving for payments is a separate and distinct problem from that of money issuance and settlement. And it is one that will undoubtedly be solved in time and only when bitcoin holders demand payments applications in greater mass, which will follow from broader adoption and the need to use bitcoin in direct commerce.

Scaling Bitcoin Is *1 to n*

If humans solved the problem of money through digital scarcity, a *0 to 1* innovation, then the technology advancements to scale transactions and ultimately solve payments are certainly *1 to n*. It is absurd to believe that human ingenuity could solve the former but then fail on the incremental derivatives. It is not just a matter of hope and faith but one of reason and logic, considering both the advancements in scaling solutions that are already being pursued and the challenges relative to the problem bitcoin has already solved. Permissionless innovation and the economic incentives inherent in bitcoin will coordinate and accelerate solutions to any number of future challenges. It takes humility to accept the magnitude of bitcoin's technological leap and to forgo the need or desire to precisely predict every next innovation or how each next problem gets solved. Market participants have an incentive to innovate to scale the network, but the solutions will have to work within the network's consensus or garner sufficient consensus to change the rules.

The nature of bitcoin's economic incentives makes it far more likely that scaling solutions work within existing consensus rules because bitcoin's value—notably its fixed supply—is predicated on its consensus rules being very difficult, if not impossible, to change. One such example is the Lightning

Network.⁵⁴ The Lightning Network builds on top of bitcoin, within the network's consensus rules, as a trust-minimized protocol to scale transaction capacity, which remains fundamentally distinct from final settlement. If successful, Lightning will be used to create a network of bitcoin payment channels between individual users and businesses that enable far greater transaction throughput at far lower cost, the scale and speed of which would rival Visa. But to be clear, even Lightning as a protocol is not an analogue to Visa, which is a company providing a service. Visa itself will likely be facilitating bitcoin transactions using Lightning in the event it is successful as a protocol. While Lightning may not be the ultimate solution, it is an example of the innovation that bitcoin is fostering. And Lightning is just one of many solutions that are actively being developed. The free market and competition will drive toward the best scaling solutions, which may be a combination of many. Importantly, however, the problem that Lightning or any other transaction-scaling protocol intends to solve is distinct from the problem bitcoin solves in issuing currency and effecting final settlement.

Protecting the Foundation at All Costs

The approach to scaling bitcoin is a slow and conservative process. Bitcoin is too important to follow the Silicon Valley mantra of “move fast and break things.” Instead, it’s “move slowly and don’t break anything.” If a global financial system is to be built on a decentralized monetary system, the foundation must be protected at all costs. Ensure the security of the base monetary layer first (bitcoin) and then allow network participants to innovate on top of it in a permissionless manner. Remember that bitcoin is only ten years old. Today, bitcoin remains at the very inception of its monetization event, and infrastructure is still being built to allow for the proliferation of this new technology and form of money.

It is a bit ridiculous to contemplate the problem bitcoin has already solved, to recognize very few people in the world yet understand it and then

⁵⁴. Joseph Poon and Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” (whitepaper, 14 January 2016).

immediately pivot to a stance of expecting mass payments here and now. Especially when considering that bitcoin, in its clearing function, is already faster and more reliable than comparable mechanisms for final settlement of dollars, euros, yen, or gold. Separately, in understanding that the fundamental use case for bitcoin today is as a long-term savings mechanism, it becomes clearer that the problem of payments is misdiagnosed and that the desired solutions can wait. In fact, bitcoin payments en masse will invariably have to wait until the market demands that solutions be created, which itself is logically dependent on more people using bitcoin as a savings mechanism. Every bitcoin user will need the ability to fulfill day-to-day payments in the future, and that day will come. In due course, we'll have our cake and eat it too. Just not at the cost of compromising bitcoin's fixed supply of 21 million, which is the *0 to 1* innovation.

CHAPTER TEN

Bitcoin Is Not for Criminals

(Originally published on 29 November 2019)

Not Inherently Criminal

If you happen to believe (or have ever heard) that bitcoin is primarily a tool used by criminals, stop and take a quick inventory of friends and family that you know or suspect may own bitcoin. How many are known criminals? While there have been widely publicized cases of criminals using bitcoin, a certain class of bitcoin skeptic assumes this must be its primary use case. The inference is generally founded upon the belief that bitcoin is inferior to the dollar, either because it is too volatile or too slow to be widely accepted for day-to-day transactions. With this flawed mental framework, the logical explanation becomes that someone would only use bitcoin to facilitate some illicit activity, generally as a means of evading law enforcement. Your favorite senator or Treasury secretary may occasionally make such a claim, but thankfully, it is not true. Bitcoin is not for criminals. It is, however, for everyone.

“The clear ends of Bitcoin for either transacting in illegal goods and services or speculative gambling make me wary of its use.”

—US Senator Joe Manchin III⁵⁵

⁵⁵. Joe Manchin III, “Manchin Demands Federal Regulators Ban Bitcoin,” press release, 26 February 2014.

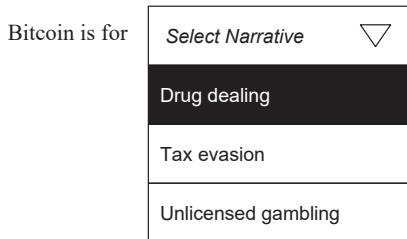


FIGURE 10.1

If bitcoin were principally used for illicit purposes, it may more logically follow that bitcoin is primarily used by criminals. Because it is not, the typical follow-on arguments that bitcoin should be banned to prevent such activity similarly do not hold water. The foundation of the idea is based on the false premise that bitcoin is inferior to the dollar when in fact, it is superior to any form of money that has previously existed, principally as a function of its fixed supply. Bitcoin's fixed supply forms the basis of the fundamental demand for bitcoin, whether it be related to criminal activity or otherwise. Without a doubt, bitcoin is most definitely used by the likes of drug dealers and other nefarious characters on the dark web. However, it would be irrational to extrapolate this as its primary use or to believe that bitcoin should be banned as a result. It is logically inconsistent to form a view that bitcoin is viable as a currency *for criminals*, while at the same time denying the implication that such a view would establish that bitcoin is functional for everyone.

Before turning the drugs narrative upside down, let's first recognize that criminals rely on any number of commonly trafficked tools and not just bitcoin: roads, the internet, the postal service, airports, the banking system, etc. All are used by criminals and often to facilitate crimes. However, criminals use each for personal, noncriminal activities too. And that is where the logic that bitcoin must be banned because it enables criminal activity completely breaks down. Crimes are crimes. There is nothing inherent in the tools used when committing a crime that makes them criminal. Using the postal service to send a letter to Mom is not a crime, but using it to send drugs is mail fraud.

Likewise, using the dollar to purchase flowers for Mom is perfectly fine, but using dollars (or bitcoin) to purchase narcotics is a crime. Despite criminal use, no one is calling for the ban of roads, the internet, the postal service, etc. And you definitely do not see any prominent defenders of the public interest calling for a ban of the dollar, which just happens to be the preferred funding currency of criminals everywhere. While fear of criminal activity has consistently been used to infringe on the rights of law-abiding citizens, believing bitcoin should be banned because drug dealers use it would be no different than calling for a ban on the dollar for the same reason.

Is Bitcoin For Criminals? Decision Tree

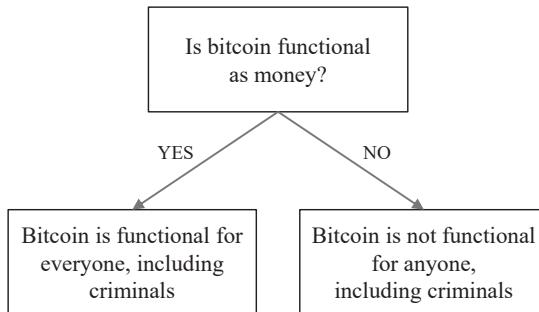


FIGURE 10.2

Missing the Point

The fact that criminals can use (and have used) bitcoin to facilitate commerce demonstrates that bitcoin can be used to facilitate any form of commerce. Any other conclusion has a logical gap and simply assumes bitcoin was used for the reason of the illicit purpose. The Silk Road, a website that facilitated transactions involving drugs and other illicit goods using bitcoin as a means of payment, was a very early and well-publicized example. However, the Silk Road merely demonstrated that bitcoin worked. But rather than focus on the more fundamental reasons why, bitcoin research often attempts to prove the counterfactual—that bitcoin is not for criminals—by establishing that only a

small percentage of bitcoin transactions facilitate illicit trade. For example, here is a recent headline from a bitcoin advocacy group:

“A new study finds less than 1% of bitcoin transactions to exchanges are illicit.”

—Coin Center⁵⁶

The substance may be true, but these counternarratives fight the battle along the wrong lines. If the Silk Road demonstrated anything, it was simply that individuals would accept bitcoin as a form of payment in return for goods and services. It does not matter that the goods sold on the marketplace were generally illicit. The Silk Road, which facilitated more than one billion dollars of transactions between almost one million users,⁵⁷ was one of the earliest demonstrations of a mass real-world use case for bitcoin. So yes, bitcoin is (and was) used for drug deals, but it is merely one use case that has helped prove bitcoin’s general utility, nothing more. And when it comes to buying drugs, the dollar remains by far the preferred method of payment over bitcoin despite all drug dealers generally being capable of accepting it. Denying that would be denying the obvious reality, but the rhetorical question to ask is “why?” Whether in response to the Silk Road or otherwise, anyone who comes away with the narrow conclusion that bitcoin works principally for illicit transactions is failing to see the forest for the trees. The more consequential and assumption-shattering implication is simply that bitcoin works. Period.

If bitcoin could work for drug dealers to facilitate commerce, could it not “work” to facilitate any other form of commerce? It does not require much imagination to carry forward the logic. If Person A would accept bitcoin for Good B, is it possible that any person might be willing to accept bitcoin for

56. Neeraj Agrawal, “A New Study Finds Less Than 1% of Bitcoin Transactions to Exchanges Are Illicit,” Coin Center, 17 January 2018.

57. US Attorney’s Office, District of Oregon, “Silk Road Methamphetamine Distributors Indicted in Federal Case Involving Four Defendants,” press release, 18 December 2013, updated 29 January 2015.

any good regardless of who or what? In the case of the Silk Road, drug dealers may not have fully understood why bitcoin “worked,” but it worked well enough that they were willing to trade drugs for it. What they seemingly understood was that there was sufficient market demand for bitcoin to make it viable as a medium of exchange. And because it provided an electronic mechanism to facilitate transactions, it opened up a market and market mechanism that may have otherwise been unavailable. Love it or hate it, it was just a market taking advantage of new technology.

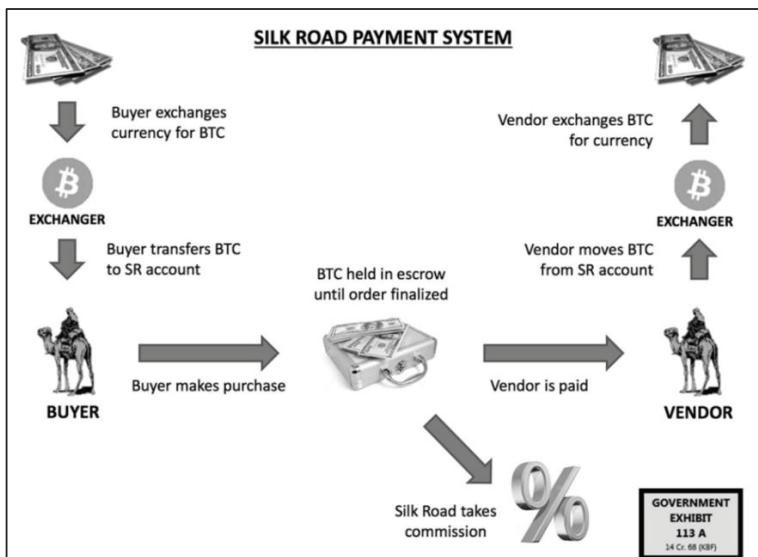


FIGURE 10.3

Source: Silk Road Payment System, government submitted exhibit in the United States of America v. Ross William Ulbricht, 2015

Despite the existence of bitcoin, drug dealers have not magically stopped accepting dollars as their preferred funding currency. Nor have they stopped laundering dollars back into the banking system. Drug dealers on the Silk Road did not use bitcoin merely to evade law enforcement, nor did the dollar drug trade suddenly disappear. Bitcoin was used because it was functional and satisfied a market need. If bitcoin were not functional and

could not be expected to hold a certain threshold of value over a particular time horizon, it would not have been used as a medium of exchange. After all, drug dealers are not in the money-losing business. But more importantly, any time anyone decries that criminals use bitcoin for illicit purposes, whether it be a US senator or a Treasury secretary, the default question to ask should be: why does bitcoin work as a medium to facilitate commerce in the first place?

The Litmus Test

Focusing on criminals distracts from the more fundamental question and consequence. If bitcoin could work for a criminal, it could work for anyone, and for bitcoin to be viable as a currency, it has to work for everyone, including criminals. However, this is not a promotion of criminal activity using bitcoin as a funding mechanism. It is merely a recognition of the properties that allow bitcoin to function in the first place. Think of criminal activity as a litmus test. If bitcoin doesn't work for drug dealers, it doesn't work for anyone. But if it works for drug dealers, it can work for everyone. If it were possible to censor (or prevent) bitcoin transactions related to certain activities or individuals, it would be possible to censor any activity and any individuals. And if there were a prime target of activities or individuals to censor, it would be that of a criminal enterprise. Such attempts have already begun.

“The U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) has sanctioned three Chinese nationals and their cryptocurrency addresses, alleging they violated money laundering and drug smuggling laws. [...] The agency also listed a number of bitcoin addresses [...] that the agency claims belong to the Chinese citizens.”

—*CoinDesk*⁵⁸

58. Nikhilesh De, “US Treasury Blacklists Bitcoin, Litecoin Addresses of Chinese Drug Kingpins,” *CoinDesk*, 21 August 2019.

Recognize that bitcoin “working” is specifically a reference to the network protocol layer. Whether a company or individual is willing to accept bitcoin from an address sanctioned by OFAC or whether a third-party financial institution freezes an account associated with such an address is of little consequence to the long-term viability of bitcoin. What is consequential is whether the network would validate a transaction originating from a sanctioned address or validate a block that includes such a transaction despite it otherwise being valid based on the network’s consensus rules—stated another way, whether bitcoin miners or nodes would reject such a transaction. Bitcoin is only viable as a currency because it has achieved a sufficient threshold of decentralization. But decentralization is not an end in itself. The end game is censorship resistance, and it is not to protect criminals. It is an end game to protect the fundamental function of the currency system.

Censorship Resistance: All or Nothing

Censorship resistance is the network’s most critical property. It ensures that the rules of the network will neither change arbitrarily nor be enforced inconsistently, without which the system would be inoperable. The most important of these rules is the finite scarcity of the currency itself. Censorship resistance reinforces scarcity, and scarcity reinforces censorship resistance. Bitcoin becomes more resistant to censorship as it scales because the network becomes more decentralized over time. As adoption increases, each individual (on average) controls an ever-diminishing share of the network’s fixed supply, and it is the scarcity of the currency which primarily drives adoption. As the network becomes further decentralized, it becomes increasingly difficult for any individual or business to censor the network. However, at any point in time, whether bitcoin is sufficiently censorship-resistant is ultimately unknown and practically unknowable. Instead, censorship resistance can only be measured through the test of time and through each failed attempt to censor the network.

From a practical perspective, the risk of censorship principally comes in two forms: forcing changes to the network's consensus rules and invalidating (or preventing) otherwise valid transactions. By design, anyone can access the bitcoin network on a permissionless basis by running a bitcoin full node. Each node can broadcast transactions to the rest of the network, and every node validates a full history of the bitcoin blockchain with each passing block based on a common set of rules.

halfin @halfin

Running bitcoin

10 Jan 2009



FIGURE 10.4

Through this operation, nodes distributed throughout the world are able to come to a common consensus regarding the valid state of bitcoin ownership across the network, on a decentralized basis and without anyone trusting any other participant. The consensus rules of bitcoin are the common language that coordinates all peers within the network, but no single party dictates the rules, and everyone opts in voluntarily. If a single party or central authority were able to force a change to the network or to influence activity within the network in such a way that would invalidate an otherwise valid transaction, it would demonstrate that the network was not sufficiently decentralized to prevent censorship.

What does all of this have to do with criminal use? If it were possible to censor criminal-related activity within the network, either by inhibiting access to the network or by preventing otherwise valid transactions from being confirmed, it would demonstrate that it is possible to censor *any* activity. The bitcoin network has no understanding of criminality or who defines it. It is amoral and apolitical. All bitcoin understands (when validating transactions) is its consensus rules. It is a closed-loop system. A bitcoin transaction

is valid if it is consistent with the network's consensus rules. If it were not, all bets would be off. If any activity within the network could be censored, it would establish that the network as a whole would be censorable, and the network's consensus rules would also be at risk.

Decentralization Spectrum

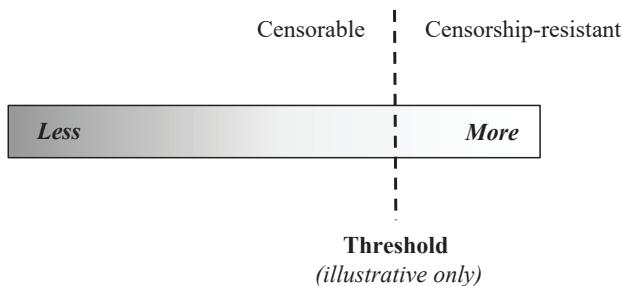


FIGURE 10.5

Censorship resistance is an all-or-nothing proposition. It either is or it is not. And if it is not, then everything is at risk, including bitcoin's fixed 21 million supply. That number and the reliability of its scarcity underpin every other economic incentive that allows the bitcoin network to function and accumulate value, including the mechanism by which the network comes to consensus. Accepting that the bitcoin network will to some extent always be used for illicit purposes is not just a libertarian bent. Instead, it is a recognition that for bitcoin to be functional and viable as a currency system, it must be so for everyone. If anyone could prevent anyone else from utilizing the network (whether it be an individual, an organization, or a nation-state), bitcoin would be at risk of failure. Censorship within bitcoin at the protocol layer is not the equivalent of PayPal deplatforming a user, nor is it akin to Bank of America closing a checking account or Visa refusing to authorize a transaction. Bitcoin is a currency issuer and settlement layer. Any effective form of censorship would undermine the system as a whole. Hence, the activity most

susceptible to censorship forms a litmus test for the rest of the network. If it were not possible to censor the most at-risk activity, it reinforces that bitcoin reliably works in all cases.

Bitcoin Is for Everyone

Ultimately, bitcoin represents a technological advancement in the global competition for money. It is the superior successor to existing fiat monetary systems, even if it is not well or widely understood today. Calling for a ban on bitcoin based on the belief that it enables criminal activity is concurrently admitting that bitcoin is functional as a currency. Consequently, if bitcoin is functional in facilitating commerce associated with illicit activities despite the best efforts of all-powerful regulatory authorities, it can be functional in facilitating any other form of commerce, including that of law-abiding citizens. It does not logically follow that its use will be confined to the dark web, nor is it today.

It is more important that innocence be protected than it is that guilt be punished, for guilt and crimes are so frequent in this world that they cannot all be punished. But if innocence itself is brought to the bar and condemned, perhaps to die, then the citizen will say, “whether I do good or whether I do evil is immaterial, for innocence itself is no protection,” and if such an idea as that were to take hold in the mind of the citizen that would be the end of security whatsoever.

—John Adams, second President of the United States⁵⁹

The competition for bitcoin is global. Over time, those that produce the most relative value will accumulate the greatest share of bitcoin. To think that those involved in illicit activities will account for a larger share of the

59. John Adams, “Argument for the Defense,” *The Trial of William Wemms, James Hartegan, William M’Cauley...for the Murder of Crispus Attucks...Superior Court of Judicature, Court of Assize, and General Goal Delivery*, Boston, 3–4 December 1770.

future bitcoin economy than today's dollar economy is not rational. And calling for a ban on bitcoin is like being afraid of your own shadow. Not only would it be impractical to enforce, but the activity such a policy would seek to prevent is enabled today in far greater proportions by the dollar. It would be analogous to throwing the baby out with the bathwater. In bitcoin, you must accept the good with the bad, recognizing that no one gets to decide due to the very nature of bitcoin. There are always trade-offs. In this case, any rational person would gladly accept that bitcoin will inevitably be used for illicit purposes as a trade-off in exchange for the economic stability that an unmanipulable global currency will provide. As with every technology, value will accrue to those who utilize bitcoin in its highest and best use, a function that only the market can determine. The net benefit will not be zero-sum. And just as the internet is not for criminals, neither is bitcoin. It is for everyone.

CHAPTER ELEVEN

Bitcoin Cannot Be Banned

(Originally published on 8 November 2019)

Is Bitcoin Functional as Money?

As individuals get closer to the precipice of understanding bitcoin as money, there is commonly an instinctive and reactionary thought that the government will never allow it. However, the idea that governments can somehow ban bitcoin is just the final stage of grief, right before acceptance. The consequence of the statement (or thought) is an admission that bitcoin “works.” In fact, it posits that bitcoin works so well that it will threaten government-run monopolies on money and that governments will regulate bitcoin out of existence to eliminate the threat. Think about the claim that governments will ban bitcoin as conditional logic. Is bitcoin functional as money? If not, governments have nothing to ban. If yes, then governments will attempt to ban bitcoin. So the anchor point for this line of criticism assumes that bitcoin is functional as money. And then, the question becomes whether government intervention could successfully cause an otherwise functioning bitcoin to fail.

As a starting point, anyone trying to understand how, why, or if bitcoin works should assess the question entirely independent of the implications of government regulation or intervention. While bitcoin will undoubtedly have to coexist alongside various regulatory regimes, imagine for a moment that governments did not exist. Would bitcoin be functional as money on a

standalone basis if left to the free market? This will inevitably lead to a number of rabbit hole questions. What is money? What are the properties that make a particular medium a better or worse form of money? Does bitcoin share those properties? Is bitcoin a better form of money based on its properties? If the conclusion becomes that bitcoin is not functional as money, the implications of government intervention are irrelevant. However, if bitcoin is functional as money, government intervention then becomes relevant to the debate. This first-order question is key for anyone evaluating whether a ban would be possible.

Banning Bitcoin Decision Tree

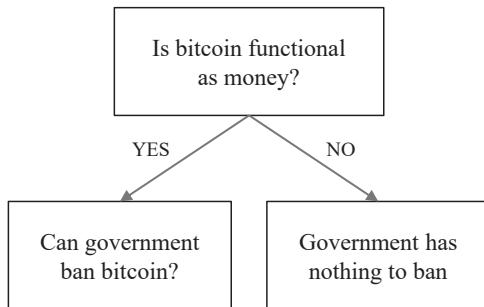


FIGURE 11.1

By design, bitcoin exists beyond governments. But it is not just beyond the control of governments. Bitcoin functions without the coordination of any central third parties. It is both global and decentralized. Anyone can access bitcoin on a permissionless basis, and the more widespread it becomes, the more difficult it becomes to censor the network. The architecture of bitcoin is practically purpose-built to resist and immunize any threats, including governments wishing to ban it. This is not to say that governments worldwide will not attempt to regulate, tax, or even ban its use. There will certainly be a fight to resist bitcoin adoption. The Fed and the Treasury (and their global counterparts) are not just going to lie down as bitcoin

increasingly threatens the government monopoly on money. However, before debunking the idea that governments could outright ban bitcoin, first understand the very consequence of the statement and the messenger.

The Progression of Denial and the Stages of Grief

The core narrative employed by the skeptic continuously shifts over time. The first stage of grief is the conclusion that bitcoin could never work and that it is backed by nothing. It is nothing more than a present-day tulip mania. With each hype cycle, the value of bitcoin rises dramatically and is then followed by a correction. Often extolled as a crash by skeptics, bitcoin fails to die, and in each instance, it finds support at levels higher than prior adoption waves. The tulip narrative becomes tired, and the skeptics move on to more nuanced issues, re-anchoring the debate. The second stage of grief follows: bitcoin is flawed as a currency. It is too volatile to be money, or it is too slow to be a payment system, or it cannot scale to satisfy all the payments in the world, or it wastes energy. The list goes on. This stage is a progression of denial and a significant departure from the idea that bitcoin lacks any substance.

While the skeptics are busy pointing out flaws, bitcoin never sleeps. The value of the bitcoin network continues its upward march. Each time bitcoin does not die, it gains strength. An increase in value is driven by a very simple market dynamic: more buyers than sellers. That is all, and it is a function of adoption increasing over time. More and more people figure out why there is fundamental demand for bitcoin and how it works. This is what creates long-term demand for bitcoin. As more people increasingly demand it as a store of wealth, there is no supply response. There will only ever be 21 million bitcoin. No matter how many people demand bitcoin, the supply side is completely fixed and inelastic. As the skeptics continue to shout the same tired lines, the crowd continues to parse the noise and demand bitcoin due to the strengths of its monetary properties. And no constituency is more well-versed in the arguments against bitcoin than adopters of bitcoin themselves.



FIGURE 11.2
Bitcoin FUD! Dice (v2) by Nic Carter (2019)

Desperation begins to kick in, and the debate re-anchors once again. The narrative predictably shifts. It is no longer that bitcoin is not backed by anything or flawed as a currency. Instead, the debate centers on regulation and government authorities. In the final stage of grief, the criticism is that bitcoin actually works too well, and as a consequence, the government will have no choice but to ban it. Really? So human ingenuity somehow reinvents money in a technologically superior medium—an achievement with mind-bending consequences—and the government is somehow going to ban that? Recognize that in claiming as much, the skeptics are admitting defeat. It is the dying whimper in a series of failed arguments. The skeptics simultaneously accept that fundamental demand for bitcoin exists and then pivot to the unfounded belief that governments can ban it.

Play this one out. When exactly would developed-world governments step in and attempt to ban bitcoin? Today, the Fed and the Treasury do not view bitcoin as a serious threat to dollar supremacy. In their collective mind, bitcoin is nothing more than a cute little toy and is not functional as a currency. The bitcoin network represents a total purchasing power of less than \$200 billion at present. Gold, on the other hand, has a purchasing power of approximately \$8 trillion (40x the size of bitcoin), and the broad money supply of dollars (M2) is approximately \$15 trillion (75x the size of bitcoin).

When does the Fed or Treasury start seriously considering bitcoin to be a credible threat? Is it when bitcoin in total represents \$1 trillion of purchasing power, \$2 trillion or \$3 trillion? Pick your number, but the implication is that bitcoin will be far more valuable and held by far more people globally by that point.

“I won’t be talking about bitcoin in ten years, I can assure you that [...] I would bet even in five or six years I’m no longer talking about bitcoin as Treasury Secretary. I’ll have other priorities.”

—US Treasury Secretary Steve Mnuchin (July 2019)⁶⁰

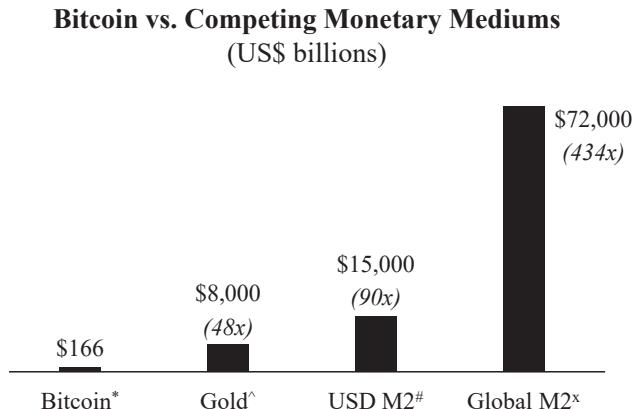
“I am not a fan of bitcoin [...], which [is] not money, and whose value is highly volatile and based on thin air.”

—US President Donald Trump (July 2019)⁶¹

The skeptic’s logic is as follows: bitcoin does not work, and if it does, the government will ban it. But governments in the *free* world will not attempt to ban bitcoin until it becomes more apparent that it is a threat. At which point, bitcoin will be more valuable and undoubtedly harder to ban, as it will be held by far more people in far more places. So, ignore fundamentals and the asymmetry inherent in a global monetization event because the government will step in to regulate bitcoin out of existence if it actually works. On which side of the fence would a rational economic actor rather be? Owning a monetary asset that has increased in value so dramatically that it threatens the global reserve currency, or forgoing ownership of that asset? Assuming an individual possesses the knowledge to understand why it is a real possibility (and increasingly a probability), which is the more defensible and logical position? The asymmetry alone dictates the former, and any fundamental understanding of the demand for bitcoin as money only reinforces the same position.

60. Steven Mnuchin, interview by Joe Kernen, *CNBC Squawk Box*, 23 July 2019.

61. Donald J. Trump (@realDonaldTrump), Twitter, 12 July 2019.



Note: M2 is an estimate of broad money supply, incl. demand deposits and time deposits.

FIGURE 11.3

Sources: *Messari, ^Unchained, #US Federal Reserve, xBloomberg. As of original publication.

An Affront to the Most Basic Freedoms

Setting all else aside, think about what bitcoin represents at an atomic level and then consider what a ban of bitcoin would represent. Bitcoin represents the conversion of subjective value, created and exchanged in the real world, for information controlled by digital keys. More plainly, it is the conversion of an individual's time into money. When someone demands bitcoin, they are at the same time forgoing demand for some other good, whether it be a dollar, a house, a car, food, or anything else. Bitcoin represents monetary savings that comes with the opportunity cost of other goods and services. Banning bitcoin would be an affront to the most basic freedoms it is designed to both provide and preserve. Imagine the response by all those that have adopted bitcoin: "Well, that was fun. The tool that the experts said would never work now works too well, and the same experts and authorities say we can no longer use it. Everybody go home. The show's over, folks." To believe that all the people in the world who have adopted bitcoin for the financial freedom and sovereignty it provides would suddenly lie down and accept the ultimate infringement of that freedom is not rational.

“Money is one of the greatest instruments of freedom ever invented by man. It is money which in existing society opens an astounding range of choice to the poor man—a range greater than that which not many generations ago was open to the wealthy.”

—Friedrich A. Hayek⁶²

Governments could not successfully ban the consumption of alcohol, the use of drugs, the purchase of firearms, or the ownership of gold. While a government can marginally restrict access or even make possession illegal, it cannot make something of value demanded by a broad and disparate group of people magically disappear. When the US made the private ownership of gold illegal in 1933,⁶³ gold did not lose its value or disappear as a monetary medium. It actually increased in value relative to the dollar, and just thirty years later, the ban was lifted. Not only does bitcoin provide a greater value proposition relative to any other good that any government has ever attempted to ban (including gold), but it is also far harder to ban given its disparate nature. Bitcoin is global and decentralized. It is without borders, secured by nodes and cryptographic keys all over the world. Banning bitcoin would require preventing open-source software from being run and preventing digital signatures (created by cryptographic keys) from being broadcast on the internet. Governments would have to coordinate across numerous jurisdictions, with the understanding that there is no way to know where the keys reside or to prevent more nodes from popping up in different jurisdictions. Constitutional issues aside, it would be technically infeasible to enforce a ban in any meaningful way.

62. Friedrich A. Hayek, *The Road to Serfdom*, condensed version (*Reader's Digest*, April 1945), 62.

63. Franklin D. Roosevelt, *Executive Order 6102—Forbidding the Hoarding of Gold Coin, Gold Bullion and Gold Certificates*, 5 April 1933.

Global Bitcoin Node Distribution (Reachable)

Snapshot: November 2019

**FIGURE 11.4**

Source: bitnodes.io

Even if all countries in the G20 coordinated to ban bitcoin in unison, it would not kill bitcoin. Instead, it would be the *fait accompli* for the fiat system. It would reinforce to the masses that bitcoin is a formidable currency, and set off a global (and hopeless) game of whack-a-mole. There is no central point of failure in bitcoin. Bitcoin miners, nodes, and keys are distributed throughout the world. Every aspect of bitcoin is decentralized, which is why running nodes and controlling keys is core to bitcoin. The more keys and the more nodes that exist, the more decentralized bitcoin becomes, and the more immune bitcoin is to attack. The more jurisdictions in which mining occurs, the less risk any single jurisdiction represents to bitcoin's security function. A coordinated state-level attack would only serve to build the strength of bitcoin's immune system. It would ultimately accelerate the shift away from the legacy financial system (and legacy currencies) and accelerate innovation within the bitcoin economic system. With each passing threat, bitcoin innovates to immunize the threat. A coordinated state-level attack would be no different.

Contrasting Monetary Systems

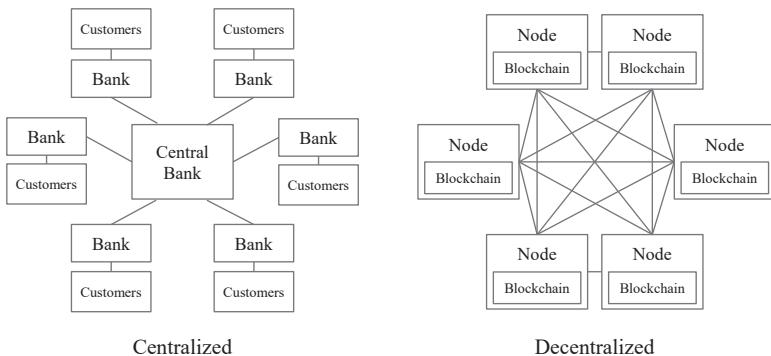


FIGURE 11.5

Permissionless innovation on a globally decentralized basis is why bitcoin gains strength from every attack. The attack vector itself causes bitcoin to innovate. It is Adam Smith’s “invisible hand” on steroids. Individual actors may believe themselves to be motivated by a greater cause, but in reality, the utility embedded in bitcoin creates a sufficiently powerful incentive structure to ensure its survival. The self-interests of millions of uncoordinated individuals, aligned by their individual and collective need for money, incentivizes permissionless innovation on top of bitcoin. Today, it may seem like a cool new technology or a nice-to-have portfolio investment, but bitcoin is a necessity even if most people do not yet recognize it. It is a necessity because money is a necessity, and legacy currencies are fundamentally broken.

Two months ago, the repo markets in the US broke (September 2019), and the Fed quickly responded by increasing the supply of dollars by \$250 billion, with more expected to come.⁶⁴ This—print money, in massive quantities—is precisely why bitcoin is a necessity, not a luxury. Bitcoin represents a step-function change innovation in the global competition for money. When an innovation happens to be a basic necessity for the functioning of an economy, no government force could ever hope to stop its proliferation.

⁶⁴. Brian Chappatta, “Fed Brings a Bazooka to Its Fight with the Repo Market,” *Bloomberg Opinion*, 11 October 2019.

And more practically, any attempt by any jurisdiction to ban bitcoin or heavily regulate its use would directly benefit a competing jurisdiction. The incentive to defect from any coordinated effort to ban bitcoin would be far too high to sustain such an agreement across jurisdictions. If the United States made the possession of bitcoin illegal tomorrow, would it slow down the proliferation, development, and adoption of bitcoin? Presumably. Would it cause the value of the network to decline temporarily? Probably. Would it kill bitcoin? No. Bitcoin represents the most mobile capital in the world. Countries and jurisdictions that create regulatory certainty and place the least restrictions on the use of bitcoin will benefit significantly from capital inflows of sound money and immigration of individuals with the foresight to save in bitcoin.

Banning Bitcoin: Prisoner's Dilemma

		Country B Bans Bitcoin (<i>cooperates</i>)	Country B Accepts Bitcoin (<i>defects</i>)
Country A Bans Bitcoin (<i>cooperates</i>)	Country B Bans Bitcoin (<i>cooperates</i>)	Bitcoin wins Ban fails, bitcoin adoption accelerates, fiat currency deterioration accelerates	Bitcoin wins Capital outflow from country A Capital inflows to country B
	Country B Accepts Bitcoin (<i>defects</i>)	Bitcoin wins Capital outflow from country B Capital inflows to country A	Bitcoin wins Everyone wins and benefits from increased trade and specialization

FIGURE 11.6

The regulatory prisoner's dilemma is not one to one. It is multidimensional, involving numerous jurisdictions with competing interests. Under these conditions, any attempt to successfully ban bitcoin becomes that much more impractical. Human capital, physical capital, and monetary capital will flow to the countries and jurisdictions with the least restrictive regulations on bitcoin. If you believe individuals will not move for freedom and opportunity, your denial is one of America. It may not happen overnight, but attempting to ban bitcoin is the equivalent of a country cutting off its nose to spite its

face. It doesn't mean that countries won't still try. India has already attempted to ban bitcoin. China has attempted to heavily restrict its use. Others will surely follow. But each time a country takes an action to restrict the use of bitcoin, it actually has the unintended effect of promoting bitcoin adoption. As it turns out, attempted bans are an extremely effective marketing tool for bitcoin. Bitcoin exists as a non-sovereign, censorship-resistant form of money. It is designed to exist beyond the state. Attempts to ban bitcoin merely serve to reinforce bitcoin's reason for existence and, ultimately, its value proposition. And in the end, every government is going to need bitcoin as money too.

Michael Goldstein @bitstein

Bitcoin is a strange game where the only winning move is to play.

14 Jan 2019



FIGURE 11.7

The Only Winning Move Is to Play

Banning bitcoin is a fool's errand. Some will try. All will fail. The very attempt to ban bitcoin will only accelerate its adoption and proliferation. It will be the hundred-mile-per-hour wind that fuels the wildfire. It will also make bitcoin stronger and more reliable, further immunizing it from future attack and reinforcing its antifragile nature. And in any case, believing governments will ban bitcoin if it becomes a credible threat to global reserve currencies is an irrational reason to discount it as a savings technology. It cedes that bitcoin is viable as money while at the same time ignoring the principal reasons as to why: decentralization and censorship resistance. Imagine understanding the greatest present secret in the world and not capitalizing on the asymmetry and utility that bitcoin provides in fear of the government. More likely, either someone understands why bitcoin works and that it will not fail at the

hands of a government, or a knowledge gap exists as to how bitcoin is able to function in the first place. Begin by understanding the fundamentals and then apply that understanding as a baseline to assess any potential risk posed by future government intervention or regulation. And never discount the value of asymmetry. The only winning move is to play.

“To govern well is a great science, but no country is ever improved by too much governing. Govern wisely and as little as possible!”

—Sam Houston,
first and third President of the Republic of Texas⁶⁵

65. Sam Houston, *The Autobiography of Sam Houston*, ed. Donald Day (University of Oklahoma Press, 1954).

CHAPTER TWELVE

Bitcoin Is Not a Pyramid Scheme

(Originally published on 18 October 2019)

Run, Don't Walk

A few years back, I received an email from a friend asking for my opinion about an investment opportunity that a mutual contact was considering. After some preliminary research, I explained that it looked like a pyramid scheme. This was my shorthand for “avoid at all cost.” I forwarded the information to our mutual contact, and the reply was not what I was expecting: “Are all pyramid schemes bad?” Yes. Of course. Some pyramid schemes are more difficult to identify than others, but even those that are easy to identify will find prey in unassuming victims. A good rule of thumb is to run, not walk, away from anything that even hints at being a pyramid scheme. While it may seem obvious, not everyone understands what a pyramid scheme is or knows the common warning signs. Ultimately, such schemes always fail.

A pyramid scheme is an investment fraud in which new participants' fees are typically used to pay money to existing participants for recruiting new members. Pyramid scheme organizers may pitch the scheme as a business opportunity such as a multi-level marketing (MLM) program. Fraudsters frequently use social media, internet advertising, company websites, group presentations, conference calls, and YouTube videos to promote a pyramid scheme.

All pyramid schemes eventually collapse, and most investors lose their money.

—US Securities and Exchange Commission⁶⁶

Not all multi-level marketing programs are pyramid schemes, but all pyramid schemes are multi-level marketing programs in some fashion. Pyramid schemes always involve some company or group of individuals selling a product for which the end demand falls far short of the available supply. The company recruits participants to purchase inventory and to recruit even more participants. The participants are all salespeople, and compensation is primarily tied to recruiting new participants rather than selling the actual product. Often the sale of the product is purposefully woven into the recruitment process. In a typical sales-driven business, the company takes on the inventory risk and pays commissions based on sales made to end users. In a pyramid scheme, the salespeople often take on the inventory risk (rather than the company), and compensation is provided for recruiting more salespeople who must then prepurchase their own inventory as part of the scheme. It all falls apart because sufficient end demand for the product does not actually exist. Everyone upstream can make money at the expense of the new recruits below them. This is a pyramid scheme. Bitcoin is not.

Bitcoin is not a company. It has no employees, and its supply is finitely scarce. No matter how many people adopt it, there will only ever be 21 million bitcoin. The distinctions should be glaringly obvious, but because bitcoin is nascent and the very nature of money is not well understood, confusion persists. Bitcoin will only become a global reserve currency if hundreds of millions (if not billions) more adopt it. And seemingly everyone that goes down the bitcoin rabbit hole ends up on the other side explaining it to their family and friends, pitching it as a better form of money. Sounds kind of like a pyramid scheme, right? Wrong. When Dell started selling personal computers via its website in 1996, and everyone told their friends

66. “Pyramid Schemes,” Investor.gov, US Securities and Exchange Commission.

to get a Dell, was it a pyramid scheme? When Apple released the first iPhone in 2007, and everyone told their friends to drop the Blackberry for its superior successor, was it a pyramid scheme?

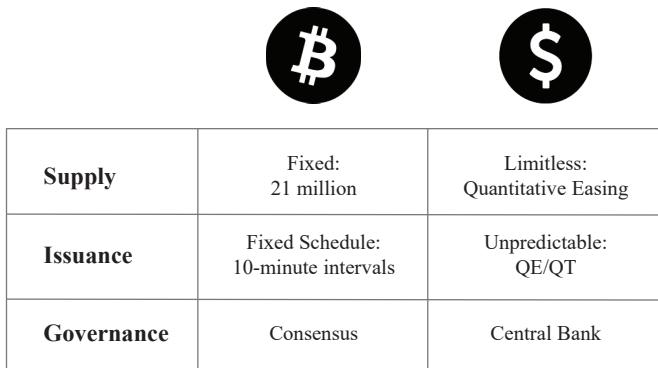
Technological shifts often happen fast. Ten and twenty years later, personal computers and smartphones are ubiquitous. It is all due to the quality of the product and the incentive structure. If someone owned shares in Dell or Apple and promoted their products, did it change the fact that the product itself provided a real value proposition? Was there a direct benefit to telling people about a new technological innovation? The value proposition of an innovation trumps all else. It does not matter how you learn about it. All that matters is whether the innovation provides utility. If it does, people will want to use it. If it doesn't, they won't.

The Utility and Innovation of Bitcoin

Bitcoin's utility is as money. It has a market because it solves a problem inherent in modern money. Not only is bitcoin not a pyramid scheme. It is fundamentally distinct from the class of innovation that any individual company could offer. Bitcoin is not Dell, nor is it Apple. It is not a tech stock. There is no corporate entity that exists behind bitcoin. Bitcoin is not a company selling a product. There are no revenues from which to pay future dividends. Bitcoin is a bearer asset. However, unlike a bearer bond, there is no income stream. Bitcoin is not about making money. Instead, bitcoin is itself money. Or at least, it has become money to those choosing to store a portion of their wealth in it. It is fundamentally about safeguarding the value you have already created—quite literally the opposite of a get-rich-quick scheme.

Bitcoin's innovation is that it represents a *superior* form of money, which is finitely scarce. There is no future promise beyond bitcoin being a form of money that no one can print. The only utility of bitcoin is in holding it as a currency and transacting with it in the future, whether that be in exchange for legacy currencies or other goods and services. It will only maintain

value if others demand it in the future, something that is true of any form of money. But money is not a collective hallucination or merely a belief system. Monetary goods have distinct properties which make them more or less effective in facilitating exchange. However, monetary properties are not absolute. The *relative* strength of monetary properties between two forms of money provides the fundamental basis of demand of one versus the other. When the market evaluates bitcoin, it does so relative to other monetary mediums, principally the dollar.



Supply	Fixed: 21 million	Limitless: Quantitative Easing
Issuance	Fixed Schedule: 10-minute intervals	Unpredictable: QE/QT
Governance	Consensus	Central Bank

FIGURE 12.1

Bitcoin is distinguished from its competition in many ways, but at its most basic surface level, supply is what differentiates at the foundation. Its supply is fixed and finite in absolute quantity, it is issued at a predictable rate in both quantity and time, and it is governed by a consensus of those who hold the currency. In a pyramid scheme, supply is functionally abundant relative to demand, and fundamental demand does not actually exist beyond that which serves to perpetuate the scheme by its organizers. Skeptics who call bitcoin a pyramid scheme (or even a Ponzi scheme, for that matter) claim it only has value if people demand it in the future, suggesting it would not have value but for a “greater fool.” Everything (and anything) needs demand to maintain value. What defines a pyramid scheme is how demand is manufactured. What differentiates sound money is the fact that a supply

constraint—it being hard to produce—is a key input to demand, which is not true of a pyramid scheme or any other type of good. The supply parameters and constraints of bitcoin are what serve as the basis for its demand. No matter how many people demand bitcoin, no more can be produced.

Supply—Fixed vs. Limitless

There is no greater contrast between bitcoin and its competition than its absolute supply. Dollars are becoming more and more abundant over time as the Fed creates trillions more with each passing round of quantitative easing, and there will only ever be 21 million bitcoin. Would an individual rather be paid in a form of money that cannot be printed or, conversely, in one whose supply is rapidly increasing in quantity over time? Humans rely on money to facilitate trade and exchange. The determinant question of which is better rests principally in the supply of the currency. A form of money that cannot be printed will preserve value better into the future than one that can. All incentives revolve around bitcoin's fixed supply.

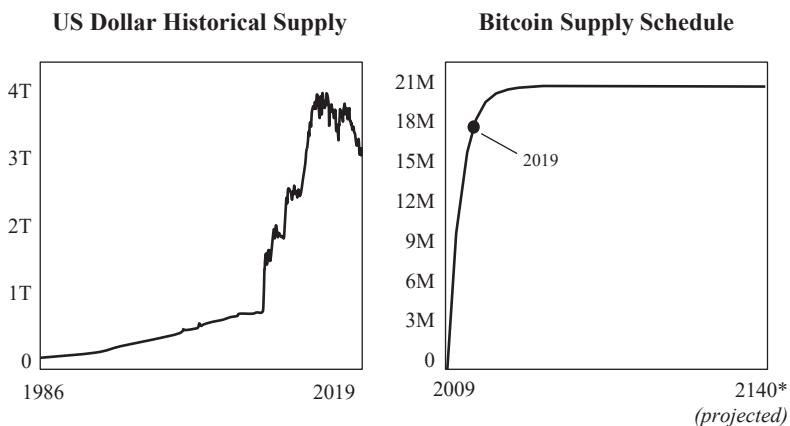


FIGURE 12.2
Source: Federal Reserve Economic Data (FRED)

Issuance—Predictable vs. Unknowable

Bitcoin's fixed supply is the foundation, but it is also issued at a predictable rate. In the future, when bitcoin reaches its maximum supply, the rate of change thereafter will be zero. But on its way to that future state, bitcoin embeds a stable and predictable supply schedule, which is a distinct and equally important part of the equation to a fixed supply. No one knows when the Fed is going to arbitrarily create more money or to what extent, in either absolute or relative terms. In contrast, bitcoin are issued through a mining process that helps secure the network, and the network adjusts to ensure that bitcoin are issued on consistent time intervals. A certain number of bitcoin are issued every ten minutes (on average). Approximately every four years, that number is cut in half until no incremental bitcoin will be issued. If more mining resources are added to the network, the network adjusts to prevent bitcoin from being issued at a faster rate. More mining results in greater levels of network security without increasing the rate of issuance or increasing the total amount of bitcoin that will ultimately be issued.

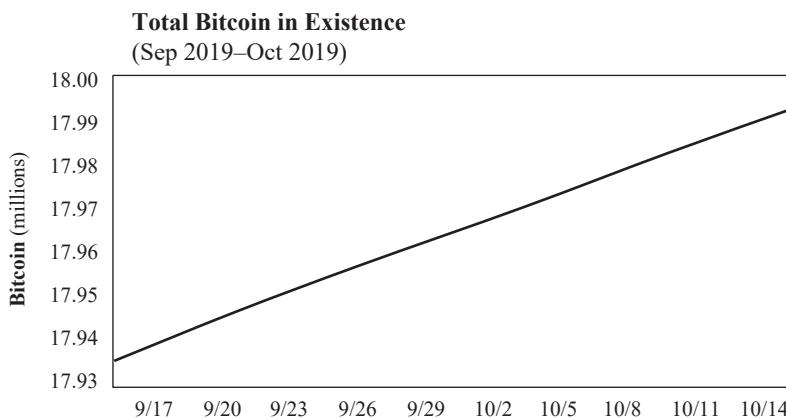


FIGURE 12.3

Source: satoshi.info

The enforcement of the issuance schedule every ten minutes, which must be consistent with a 21 million terminal fixed supply to be valid, builds increasing credibility in the future state supply. All market participants come to understand that the fixed supply will be enforced, not because of a magical point in time when the maximum is reached, but as a result of the network enforcing its monetary policy every ten minutes. This rigidity allows the entire economic system to plan for the future. Miners building security infrastructure are able to forecast future compensation, and all market participants can know the rate of change of the currency at any point in time.

Governance—Monetary Policy by Consensus vs. Central Bank

By running a bitcoin full node, anyone can verify the number of valid bitcoin in circulation and the amount of new bitcoin issued in each block without trusting anyone else. Through this same process, the consensus of nodes actually enforces both the fixed supply and the issuance schedule at the same time. Everyone can approximate with precision when the issuance rate will be reduced and validate that it has in fact occurred with their own node. Technically, enforcement occurs every ten minutes, six times an hour, 144 times a day, 4,320 times a month, and 52,560 times a year, with each passing bitcoin block that is accepted as valid. As blocks are propagated throughout the network, each node either accepts the block as valid or rejects it as invalid. Any block that includes an amount of bitcoin to be issued inconsistent with the fixed supply is independently rejected by each node. That is enforcement, but each node can also validate at any point in time that the circulating supply and the issuance is consistent with the fixed supply of 21 million. The monetary system hardens as more market participants validate and enforce the monetary policy of the network, over and over again, every ten minutes.

The consensus mechanism that governs bitcoin is the foundation of its credibility and what ultimately sets bitcoin apart from its competition. In

the central banking monetary model, twelve individuals (or thereabout) determine how and when to create billions, if not trillions, of dollars. Bitcoin, on the other hand, entrusts its monetary policy to a consensus mechanism of those that hold bitcoin as a currency. Even if an individual were to remain unconvinced that a currency with a fixed supply issued at a predictable rate is superior to one with an unpredictably inflating supply, it does not matter what any individual believes. If the market collectively determined that it would be better to remove the fixed supply cap, it is theoretically possible. However, to do so, a decentralized network (without any central coordination) would have to reach an overwhelming consensus to debase a currency that has been adopted principally for the reason that it cannot be printed. Bitcoin ultimately represents the contrast between monetary policy by consensus and monetary policy by central bank. Nothing occurs by dictate. The consensus of the network enforces the fixed supply, and everyone has an incentive to ensure that no one else can create more units of the currency arbitrarily.

Verification of Bitcoin Supply and Issuance Rate on a Bitcoin Full Node (Block Height: 599,114)

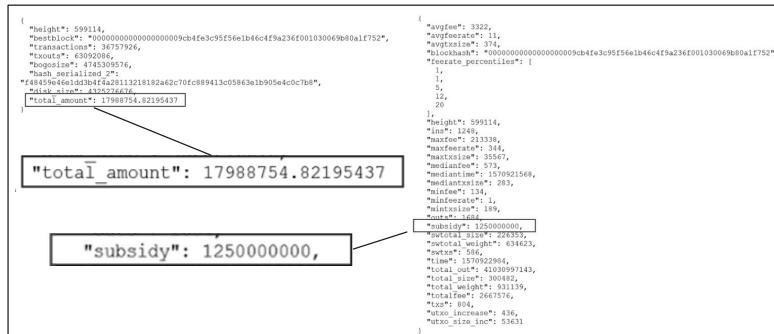


FIGURE 12.4

Bitcoin Is Not a Pyramid Scheme

So no, bitcoin is not a pyramid scheme. It is not organized by a sketchy company, pushing high-pressure sales tactics. It is not peddling some inferior consumer good with an abundant supply, where compensation is directly tied to recruiting new members to the scheme. Bitcoin is money, and its supply is finitely scarce. Its supply remains wholly unaffected by the level of adoption. The same pie is simply divided across more participants as adoption increases. And on average, more people control a smaller share of the network. Its value increases as a function of adoption, and adoption increases because its monetary properties are superior to the competition. Bitcoin has a fixed supply, its supply schedule is predictable, and its monetary policy is governed and enforced by consensus. Everything changes around bitcoin, but bitcoin's fixed supply remains the constant.

Just because people who adopt bitcoin as money often advocate for it does not make it a pyramid scheme. Imagine you concluded that bitcoin is a superior form of money and that there is a fundamental and acute problem with central banks creating money arbitrarily out of thin air. Would you hide this secret from your friends and family? The skepticism for advocacy of bitcoin is healthy, but recognize that bitcoin adoption can only grow through education. If there is a moral case to educate your friends and family—which there is—it logically extends beyond that. But advocacy is not just altruistic. Most people struggle to grasp the properties that define money or to see how these properties exist in bitcoin. In many ways, bitcoin is not just a secret hiding in plain sight. It is the greatest secret that exists in the world. Once someone figures it out, often after years of denial and financial opportunity cost, it is perfectly logical to want to help others figure it out too. Some things are too good to keep secret, and there is a long-term incentive for each holder of the currency if more people adopt it. Bitcoin becomes more secure, and its utility as money increases with greater adoption.

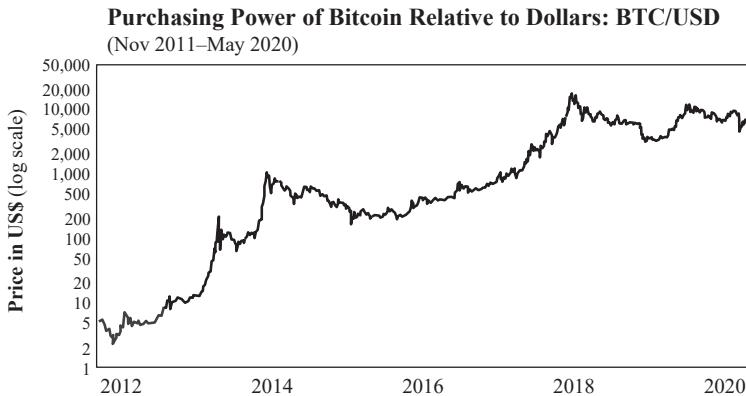


FIGURE 12.5

Source: Bitstamp

At the end of the day, the value of bitcoin is not dependent on any single individual figuring it out and buying in. An objective truth either exists in the world, or it does not. Bitcoin either has a fixed supply, or it does not. If it does, it will be adopted by the entire world as money. If there were more people wanting to sell their bitcoin than people needing to adopt bitcoin as money, then its price and value would decline over time. Regardless of all the people who turn into advocates for bitcoin after having adopted it or why the phenomenon exists, neither can obfuscate a fundamental economic fact, especially over the course of a decade. Knowledge distributes as a function of time. If bitcoin's supply were not credibly fixed and if early adopters sold their bitcoin in a proportion greater than the rate of new adoption, bitcoin would not be viable as money, and its value would trend to zero rather than increase to higher and higher levels. Always anchor to the fundamentals. Why does fundamental demand exist, and is it because bitcoin is finitely scarce? If so, there is a fundamental explanation for its demand, demand will far outstrip supply, and bitcoin is not a pyramid scheme.

PART III

Bitcoin vs. the Dollar

CHAPTER THIRTEEN

Bitcoin Fixes This

(Originally published on 30 August 2019)

Jackson Hole

Each year central bankers, establishment economists, and talking heads from around the world descend on Jackson Hole, Wyoming to discuss the systemic issues that plague *our* economy. Constantly searching for an answer but never seeming to find one. It is the perennial Jackson Hole dilemma. There is always much fanfare, and the 2019 edition was no different. Lawrence Summers, former US Treasury secretary and former president of Harvard University, may have best summarized, and inadvertently exposed, the issue with the whole spectacle in a twenty-eight-part tweet thread.⁶⁷ Summers questioned a number of foundational assumptions made by the establishment economic mainstream, of which he is a resident member, and also identified many symptoms of economic instability that have become increasingly systemic.

The fundamental question from Summers: can central banking, as we know it, be the primary tool of macroeconomic stabilization in the industrial world over the next decade? Summers doubts that it can. However, he still could not be further from the target. The monoculture of economic thinking in the US believes central banking has a fundamental role to play

⁶⁷. Lawrence H. Summers (@LHSummers), Twitter, 22 August 2019.

in creating economic stability. Not just *a* role but a fundamental one. What tools to use, how, when and to what degree it will be effective is the debate. Central banking is assumed at a foundational level as necessary to achieving economic stability. Even in Summers's own words, the question "Can central banking be the *primary* tool?" carries that built-in assumption, with primary being the key word. What the mainstream, including Summers, does not question—nor is it capable of questioning—is whether central banking *is* the problem rather the solution. Whether it is the primary cause of macroeconomic instability rather than a source of stability.

Lawrence H. Summers @LHSummers

Coming into Jackson Hole, economists are grappling with a major issue: Can central banking as we know it be the primary tool of macroeconomic stabilization in the industrial world over the next decade? In my forthcoming paper w/ @annastansbury, we argue that this is in doubt. 1/

22 Aug 2019



FIGURE 13.1

Historical Track Record

As a historical record, since the financial crisis, central banks have used quantitative easing as the primary tool to help stabilize the economy. Quantitative easing, or QE for short, is a term used to describe the operation of central banks increasing the money supply to "ease" financial conditions. The playbook is as follows: increase the money supply, reduce interest rates, manufacture price inflation, and reflate asset values such that existing debt levels can be sustained and more debt can be created. While central banks use many technical terms, increasing or decreasing the money supply is really the only tool in the tool kit to manipulate interest rates and to effect directional shifts in asset prices.

The Central Bank Playbook

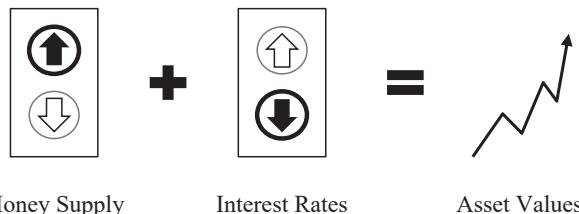


FIGURE 13.2

Despite record-low interest rates today, the global economy has once again begun to deteriorate. Naturally, many are questioning the effectiveness of quantitative easing. What has long been taught as axiomatic is now very much in doubt, but again, there is a critical difference between questioning effectiveness and recognizing that the perceived solution is actually the problem. When taking a closer look into how quantitative easing works, and its consequences, it becomes clear that the function of quantitative easing actually creates the instability it seeks to prevent. It is made worse by the fact that central bankers who have this immense power go back to the same well, time and again, despite having been proven wrong on a wide range of the most consequential matters and without any real function of accountability.

“The risk that the economy has entered a substantial downturn appears to have diminished over the past month or so.”

—Ben Bernanke, former chair, US Federal Reserve, June 2008⁶⁸

Ben Bernanke famously made this comment three months before Lehman Brothers failed and the first of three formal rounds of QE was introduced as a response to the Great Financial Crisis. QE1, QE2 and QE3 increased the money supply by \$1.3 trillion, \$0.6 trillion, and \$1.7 trillion, respectively. In total, the Fed introduced \$3.6 trillion new dollars into the banking system via

68. Ben Bernanke, “Outstanding Issues in the Analysis of Inflation” (speech), Federal Reserve Bank of Boston’s 53rd Annual Economic Conference, 9 June 2008, Chatham, MA.

QE from 2009 to 2014, quintupling the size of its balance sheet or increasing the base money supply fivefold.⁶⁹ The merits can be debated but the facts are the facts. Following the crisis, the Fed pursued QE on three separate and distinct occasions, each time in an attempt to stabilize the economy. Setting the technical jargon aside, it is all just money printing. If at first you do not succeed, print more money to stabilize the economy.

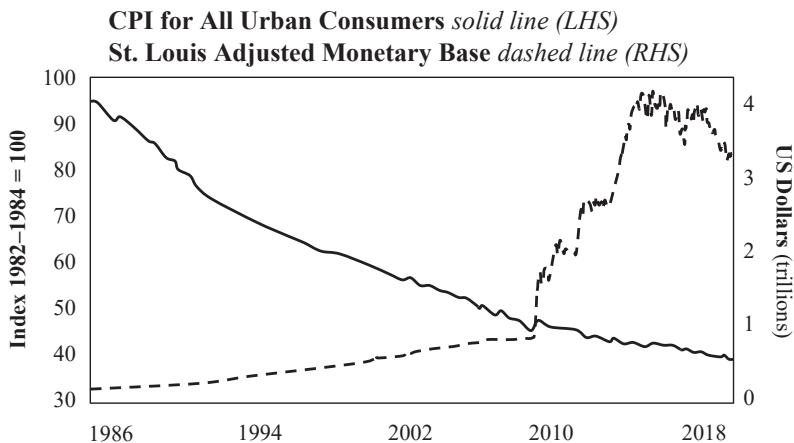


FIGURE 13.3

Source: US Bureau of Labor Statistics and Federal Reserve Economic Data (FRED)

While QE isn't technically "printing money," the result is functionally the same. The Fed digitally creates new dollars on a ledger (literally out of thin air) and proceeds to use those dollars to purchase financial assets, such as US treasuries (government debt) and mortgage-backed securities. As a net effect, more dollars exist within the banking system in the form of bank reserves that can then be used to lend or purchase other assets. In simple terms, more dollars exist, which causes the value of each individual dollar to decrease. However, the effect is not direct. Instead, it is transmitted gradually through the expansion of the credit system. Said another way, QE creates more dollars and allows

69. Federal Reserve Bank of St. Louis, "Adjusted Monetary Base (DISCONTINUED)," retrieved from Federal Reserve Economic Data (FRED), Federal Reserve Bank of St. Louis, August 2019.

banks to expand credit by multiples of each dollar created. This incremental credit (i.e., auto loans, mortgages, student loans, etc.) is then used to purchase goods in the real economy. However, creating money out of thin air does not magically create more goods and services. More base money exists and even more deposits exist as credit is created, which compete for a supply of goods and services that do not and cannot keep pace. That causes the value of the dollar to decline on a relative basis.

Does Quantitative Easing Work?

People often ask whether quantitative easing *works*. The short answer is no. While many believe that QE was necessary, it merely kicked the can down the road and guaranteed more QE would be necessary in the future. The root cause of the financial crisis was a financial system that had become far too leveraged. At the time, every dollar in the banking system had been leveraged and lent 150:1.⁷⁰ There was too much debt and too few dollars. This degree of leverage was only made possible as an indirect function of the Fed sustaining economic imbalances. With every recessionary business cycle in the decades leading up to the crisis, the Fed increased the supply of dollars to lower interest rates and induce credit expansion—similar in operation to post-crisis QE, just much smaller and more gradual. Rather than allow the system to course-correct and reduce the amount of debt as a natural market function, the Fed's continual response was to provide more dollars in order to sustain existing debt levels and permit further credit creation.

Through this course of action, the Fed inadvertently created the fragility and instability that existed in the financial system in 2008. By pursuing continual credit expansion, an unsustainable degree of system leverage was allowed to accumulate over the course of several decades. While similar policies had been pursued before, the financial crisis created an environment

70. Board of Governors of the Federal Reserve System, *Z.1 Financial Accounts of the United States: Flow of Funds, Balance Sheets, and Integrated Macroeconomic Accounts, First Quarter 2019*, Federal Reserve Statistical Release, 6 June 2019, 7.

that triggered a more drastic response from the Fed. Simply put, the Fed needed a bigger boat. For context, the cumulative increase in the money supply through QE1, QE2, and QE3 of \$3.6 trillion over the five years following the crisis was 36x larger than the \$100 billion increase in the five years prior to 2008. This time *was* different. The real issue was the sustained imbalances in the credit system accumulated over many cycles and the overall degree of leverage. Eventually, the bubble was destined to burst. An exogenous shock to the system was inevitable as a function of time and as the problem became worse with increasing size.

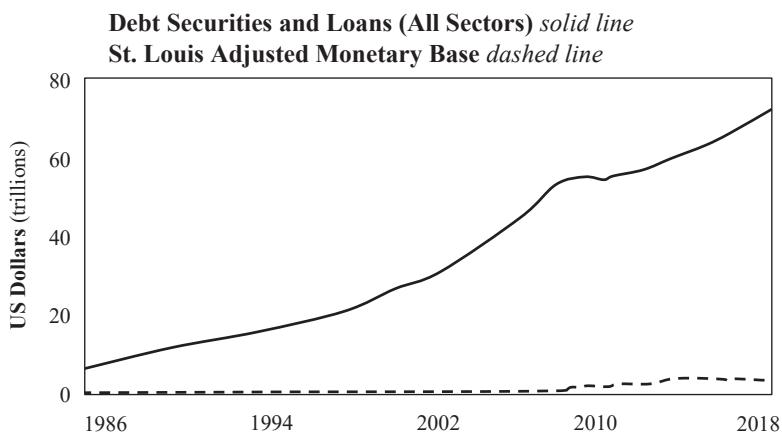


FIGURE 13.4
Source: Federal Reserve Economic Data (FRED)

In the Fed's economy, the credit system became orders of magnitude larger than the amount of base money that existed. As a result, the credit system became the marginal price-setting mechanism rather than the base money. Because the Fed has a mandate to maintain price stability, it must implicitly maintain the size of the credit system in order to sustain general price levels. During the financial crisis, the credit system began to collapse, and asset price levels rapidly declined in a disorderly fashion. To reverse the impact, the Fed was forced to drastically increase the money supply to maintain the size of the credit system, in a way it never had before. However, even after the

height of the crisis, the Fed determined it was necessary to add trillions more in new dollars post-QE1 to continue to support a languishing system, despite acknowledging the limitations of its monetary policy tools. This is the Fed's Catch-22. Even when it seemingly knows better, the default position is to err on the side of more QE, not less. To try again what has not worked in the past to achieve stability. It is the definition of insanity.

“I’m perfectly willing to accept the argument that monetary policy is not the main tool, that this is not the main thing wrong with the economy, but it’s our duty to do what we can, to be palliative, to help where we can, even if we can’t solve fiscal, structural, and other problems.”

—Ben Bernanke, former Fed chair, August 2011⁷¹

“I don’t think it is literally the case that monetary policy is completely ineffective. I think we can see the effects on financial markets, which in turn must be affecting wealth, confidence, and some other determinants of spending and production. To the extent that transmission is weaker, that could be used to argue for more stimulus rather than less stimulus.”

—Ben Bernanke, former Fed chair, September 2011⁷²

By responding with QE, the Fed induced a credit system already saddled with unsustainable amounts of debt to expand massively. Today, the US credit system supports approximately \$73 trillion of fixed-maturity debt systemwide, representing an increase of \$20 trillion (+40%) above pre-crisis levels (see Figure 6.4). This debt is stacked against only \$1.7 trillion of actual dollars that exist within the banking system and \$3.8 trillion in total

71. *Minutes of the Federal Open Market Committee*, a joint meeting of the Federal Open Market Committee and the Board of Governors of the Federal Reserve System, Washington, DC, 9 August 2011.

72. *Minutes of the Federal Open Market Committee*, a joint meeting of the Federal Open Market Committee and the Board of Governors of the Federal Reserve System, Washington, DC, 20–21 September 2011.

circulation.⁷³ After years of increasing the money supply, the Fed pursued a reverse operation, gradually reducing the supply of dollars from September 2017 to today. Consequently, there is far too much debt and too few dollars. Because QE induces the creation of ever-increasing amounts of debt, it is more like heroin than an antibiotic. The more that is applied to a financial system, the greater the dependency that develops and the worse off that system becomes when QE is withdrawn. The rhetorical question to ask is: if QE works, why does the Fed always need another round? QE only leads to more QE. Money printing begets money printing, and it is the best empirical evidence to demonstrate that QE does not “work” by any measure.

Bitcoin Fixes This

Prior to 2009, everyone was forced to opt in to this increasingly fragile system as there was no viable off-ramp. The advent of bitcoin, which was launched during the crisis, provided the first credible alternative to opt out, and it exists largely as a response to global QE. While bitcoin would have represented a superior alternative to fiat currencies even in the absence of QE, the global monetary debasement in response to the crisis sharpens the contrast. It is this contrast that makes bitcoin far more intuitive. Bitcoin might technically exist because some highly intelligent individuals identified a problem and set the wheels in motion to create a solution, but it functionally exists because it fixes the problem of printing money.

Given the existing leverage that persists in the financial system, future QE from the Fed (and central banks worldwide) is not merely a possibility. It is a certainty. The credit system was unstable and unsustainable in 2008. As a function of QE, it has expanded massively and now supports \$20 trillion more debt in the US alone. Every time the Fed, or any central bank, announces subsequent rounds of QE, it reinforces to the market why bitcoin exists. It also establishes that QE does not work. Market participants are

73. Board of Governors of the Federal Reserve System (US), *H.8: Assets and Liabilities of Commercial Banks in the United States*, Federal Reserve Statistical Release, 29 August 2008.

presented with the choice between holding a form of money that is continually and systematically debased by central banks or a form of money with a fixed supply that cannot be printed. Bitcoin is the check, balance, and ultimate opt-out path to the problem QE presents. Bitcoin cannot prevent the printing of dollars, but it is a solution to the same problem.

In “The Pretense of Knowledge,” a speech delivered by Friedrich Hayek at the ceremony awarding him the Nobel Prize in Economics in 1974, Hayek articulates the first principles of why the disparate knowledge of all market participants is greater than that possessed by any single mind. He explains why the dominant macroeconomic theory and monetary policy that guide central banks are inherently flawed through the same reasoning—and why the policy tools used by central banks, such as quantitative easing, create more harm than good.

In fact, in the case discussed, the very measures which the dominant “macro-economic” theory has recommended as a remedy for unemployment, namely, the increase of aggregate demand, have become a cause of a very extensive misallocation of resources which is likely to make later large-scale unemployment inevitable. The continuous injection of additional amounts of money at points of the economic system where it creates a temporary demand which must cease when the increase of the quantity of money stops or slows down, together with the expectation of a continuing rise of prices, draws labor and other resources into which can last only so long as the increase of the quantity of money continues at the same rate—or perhaps even only so long as it continues to accelerate at a given rate. What this policy has produced is not so much a level of employment that could not have been brought about in other ways, as a distribution of employment which cannot be indefinitely maintained and which after some time can be maintained only by a rate of inflation which would rapidly lead to a disorganization of all economic activity.

—Friedrich A. Hayek⁷⁴

⁷⁴. Friedrich A. Hayek, “The Pretense of Knowledge,” Lecture in the Memory of Alfred Nobel, 11 December 1974, Stockholm, Sweden.

The speech in its totality, including this excerpt, provides the counter-narrative to the monoculture of today's economic policymaking. In short, our current system entrusts the allocation of trillions of dollars to just a few individuals. It is not that these individuals lack a significant amount of knowledge. Instead, it is that any small group of individuals necessarily possess far less knowledge than the market of all people who actually make up an economy. Attempting to manage an economy by manipulating the money supply effectively replaces the knowledge of the entire market with that of just a few individuals. The mechanisms that govern supply and demand can no longer function efficiently, which creates imbalances that can only be sustained so long as the market remains manipulated. The financial crisis is patient zero, and the QE response has only left us in a more precarious situation than before. The first-order impact is the devaluation of the currency, but the broader, longer-term impact is the deterioration of the underlying economic structure as a whole.

“I don’t believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can’t take them 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 A. Hayek⁷⁵

Bitcoin may just be the sly roundabout way around the Fed’s economic system that Hayek theorized. Bitcoin creates a system that allows for undistorted economic activity, and it achieves this through a fixed monetary supply governed by a market consensus mechanism. Through this consensus mechanism, bitcoin dispenses with the need for the conscious control of central bankers, relying instead on the distributed knowledge of all market participants. It is also completely voluntary. If you like your financial system, you can keep it (at least for now). However, economic systems converge on

75. Friedrich A. Hayek, “Exclusive Interview with F.A. Hayek,” interview by James U. Blanchard III, University of Freiburg, Germany, 1984.

a single form of money.⁷⁶ And as individuals increasingly opt in to bitcoin, it will only make the issues present in the legacy system more evident. The greater the inclination to store wealth in bitcoin, the lesser the demand to store wealth in the dollar or assets that support the existing dollar credit system. In essence, an increasing shift to bitcoin will impair the supply and demand for dollar credit, accelerating the need for the legacy financial system to rely on even more QE to sustain itself.

While not popular and certainly not accepted by Summers's Jackson Hole crowd, there is an opposing economic view that argues the very function of a central bank and its active management of the money supply is harmful to the economy. Practically speaking, this view cannot coexist within a central bank because it is antithetical to its primary function. It is why the monoculture came to be and why a different course is never charted. Now that bitcoin exists, however, the monoculture is being challenged credibly for the first time in a long time, and it is no longer merely the subject of an intellectual debate. It is a market test. Two competing monetary systems exist that present a great contrast: one attempts to create stability through active management of the money supply, while the other tolerates interim volatility in the interest of maintaining a fixed supply. Bitcoin provides a credible path to opt out of the legacy system that did not previously exist. It may be volatile, but bitcoin adoption will continue to increase principally for the reason that it represents an alternative that eliminates the ability to create money and actively prevents quantitative easing, the primary central banking policy tool that creates economic instability.

76. Reference the essay titled "Bitcoin Obsoletes All Other Money" for a fundamental discussion of why money converges on one medium.

CHAPTER FOURTEEN

Bitcoin Is a Rally Cry

(Originally published on 26 March 2020)

A Fundamental and Inalienable Right

| “To the People of Texas and all Americans in the world.”

—Lt. Colonel William B. Travis, February 1836⁷⁷

In his open call to arms from the Alamo, Lt. Colonel William B. Travis began with an expression of America as an idea extending beyond borders, to “all Americans in the world.” It was a plea to all those who valued the fight for liberty and freedom. Outnumbered ten-to-one, Travis responded to the demand for surrender with a cannon shot. He was no more than twenty-seven years old at the time. Texas declared its independence a week later, but within days, the Alamo fell. The Travis letter became the rallying cry of a revolution. Remember the Alamo. Ultimately, Texas won its independence. Always outnumbered, it is a reminder that the endless pursuit of freedom is a most powerful equalizer. And it is something inherent to the character of all *Americans* in the world. Not just American citizens but everyone who values individual liberty.

Minus the lionized heroes and a literal declaration of independence, bitcoin is still very much a fight for freedom. It is becoming a rallying cry to

77. William Barret Travis, “To the People of Texas & All Americans in the World,” an open letter from the Alamo, 24 February 1836.

all those that refuse to sit back and accept the fate of our tenuous financial system. The very idea of freedom may be the single most important tenet underpinning the monetary revolution to which bitcoin is giving rise. When the war is won, bitcoin will likely find its way into a constitutional amendment even though the first amendment already covers it—the right of the people to keep and bear bitcoin. Prior to bitcoin, there was no practical choice but to opt in to a broken currency system. That all changed in 2009 when bitcoin was released into the wild. Controlled by no one, bitcoin is an entirely voluntary system. It affords everyone the ability to store and transfer value in a currency that cannot be manipulated. Bitcoin may not be synonymous with the right to life, liberty, and the pursuit of happiness, but it is a fundamental and inalienable right for those who choose to rely upon it as a better path forward.

While bitcoin is valued for different reasons, it consistently appeals to those that have identified the inherent level of freedom afforded by such a powerful tool, particularly in a world full of never-ending economic calamities. As the fragility and instability of the global financial system become more apparent by the day, central bankers and politicians scramble in a race to see who can provide more stimulus to an economy that is flatlining. Lest we forget, the instability in the financial system is not just appearing. It is reappearing. The structural issues now resurfacing are the same ones that existed during the 2008 financial crisis. Before the oil war and the global pandemic in 2020, the repo funding markets broke in September 2019.⁷⁸ The writing was not just on the wall. It was in the repo markets. If it were not these recent events acting as the accelerant, it was inevitable that an exogenous shock would expose what remained under the surface all along—a highly leveraged financial system primed to break at the first signs of any material stress.

78. Summer Said and Benoit Faucon, “Inside Saudi Arabia’s Decision to Launch an Oil-Price War,” *Wall Street Journal*, 10 March 2020; Liz Capo McCormick and Alexandra Harris, “The Repo Market’s a Mess. (What’s the Repo Market?),” *Bloomberg News*, 19 September 2019.

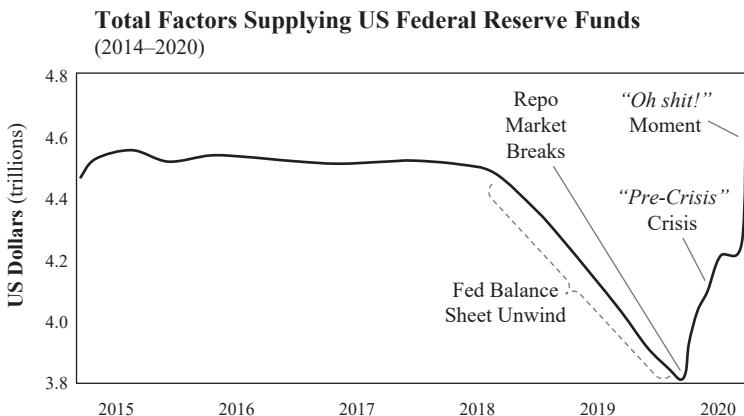


FIGURE 14.1
Source: Federal Reserve Economic Data (FRED)

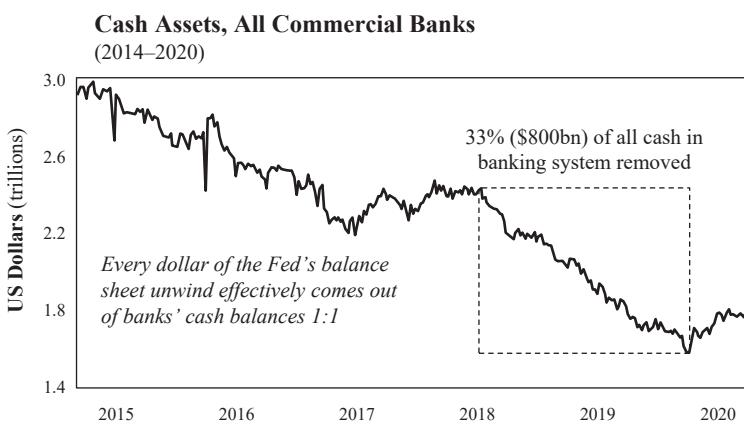


FIGURE 14.2
Source: Federal Reserve Economic Data (FRED)

A Game of Guess and Check

From October 2017 to September 2019, the Fed reduced the supply of dollars in the US financial system by \$700–\$800 billion, effectively reducing the cash available in the banking system by 33%, in an attempt to unwind post-2008 financial crisis quantitative easing. The Fed functionally starved the financial system of liquidity it needed to function, which ultimately

caused the repo markets to break. This is what induced the need to rescue financial markets initially six months ago (in September 2019). Prior to the global economic shutdown, the Fed had already supplied ~\$500 billion in emergency funding to the repo markets to quell market turmoil. But matters have since materially worsened, and now the fuel is really being dumped on the proverbial fire. It is not just the scale that is alarming but the clear demonstration of control being lost through a meandering path of incrementalism. After the stock market crash in late February 2020, the Fed issued an emergency 50 bps interest rate cut. The market then cratered further, and the Fed responded with an incremental \$1.5 trillion in short-term funding (one to three months) to be supplied in the repo markets. The market crashed yet again, and three days later, the Fed announced a formal \$700 billion “quantitative easing” program to purchase \$500 billion in US government treasuries and \$200 billion in mortgage-backed securities. Coinciding with this move, short-term interest rates were cut by 100 bps, down to zero.

Yep, you guessed it. The market crashed again. Credit markets became dislocated, and the Fed followed with a “whatever it takes” response, announcing an unlimited QE program.⁷⁹ Its three most aggressive moves to date all transpired within a ten-day window. And as part of its latest unprecedented act, the Fed will begin buying corporate bonds on the secondary market while also participating in the primary issuances of corporate credit. It also expanded its purchases of mortgage-backed securities to include commercial mortgage-backed securities (commercial real estate). In addition, the Fed established a facility to issue asset-backed securities in order to purchase student loans, auto loans, credit card loans, etc. All this without a price tag and just a promise to do whatever it takes. It would be funny if it weren’t so serious. But the real question remains: if the Fed were in control, why was it so reactionary? Why did its plans change so drastically in a ten-day period if it genuinely understood the extent of the issue? Never mind the unintended

79. Board of Governors of the Federal Reserve System, “Federal Reserve Announces Extensive New Measures to Support the Economy,” press release, 23 March 2020.

and unknowable consequences. It merely demonstrates that the Fed is not in control. Why would it have announced a \$700 billion QE program if it didn't expect it to work? It is a classic game of guess and check, except the consequences can never be checked (only the immediate market reactions). The problem is that the entire US economy is at stake.

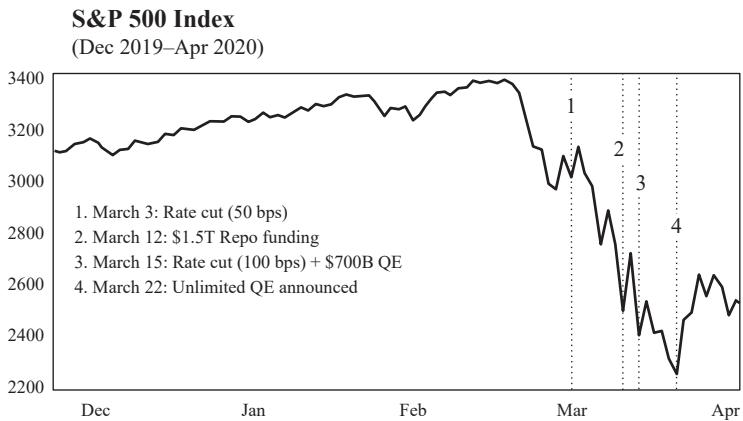


FIGURE 14.3

Source: S&P Dow Jones Indices

“There’s an infinite amount of cash at the Federal Reserve.”

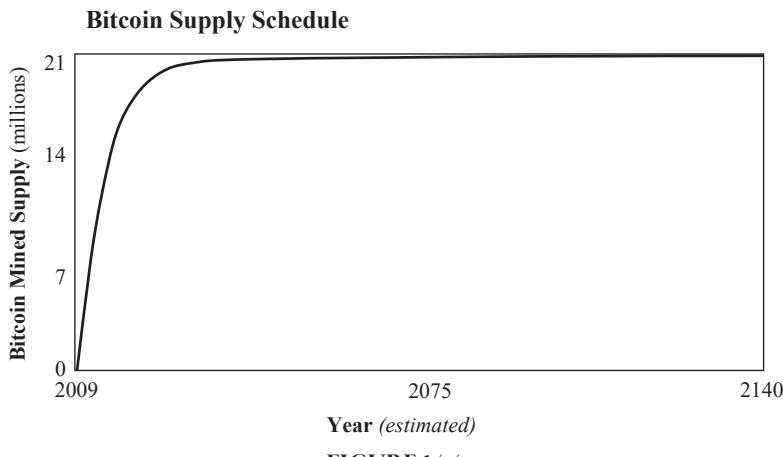
—Neel Kashkari,
president, Federal Reserve Bank of Minneapolis, March 2020⁸⁰

“To lend to a bank, we simply use the computer to mark up the size of the account they have with the Fed, [...] it’s much more akin to printing money than it is borrowing.”

—Ben Bernanke,
former chair, US Federal Reserve, March 2009⁸¹

80. Neel Kashkari, “Coronavirus and the economy: Best and worst-case scenarios from Minneapolis Fed president,” *60 Minutes*, Interview, 22 March 2020.

81. Ben Bernanke, “The Chairman: Part 1,” interview by Scott Pelley, *60 Minutes*, 15 Mar 2009.

**FIGURE 14.4**

The New Normal

Make no mistake. The \$1.5 trillion supplied to the repo markets will be converted to increment the Fed's formal quantitative easing program, and the entire unquantified program should conservatively be expected to exceed \$4 trillion when all is said and done. The Fed cannot put out the fire that is a liquidity crisis through short-term funding. It will have no choice but to monetize a larger share of the credit system than it did in 2008 because the problem is now larger. In addition, while not yet passed as of the time of writing, Congress is working on an initial \$2 trillion stimulus package in response to the global pandemic. With a market already suffering a liquidity crisis, the banking system does not magically have this cash on hand to finance a massive expansion of the federal government's deficit. As a result, the Fed will be forced to finance any fiscal response through an ever-expanding quantitative easing program. It is the only way for the banks to get the cash needed to finance such a fiscal stimulus. All roads lead back to the Fed and endless QE.

As the world looks on, amidst the fear and panic, it often seems like there is no alternative. While it's unclear precisely when so many people began to

view the government's role as one of fighting global pandemics (rather than the free market), that is the world aggressively being demanded by many. It is a symptom of failing to understand the root problem. Misdiagnosing the fallout of a global pandemic—and falsely believing the only hope is to allocate money created out of thin air by central banks and governments—is predictably irrational. There is no reason that even a few months of complete economic shutdown should put the world on the brink of a global depression. Instead, it is the output of an inherently fragile financial system, one that is dependent on perpetual credit expansion and would collapse without it. The fragility of the global financial system itself is the problem, not a global pandemic. Do not be fooled. The present instability is not a pandemic-induced failure of the financial system. Failure was an inevitability, pandemic or not.

The world would not be waking up to the S&P 500 futures locked “limit-down” with seeming regularity if not for its heavy dependence on credit and an unsustainable degree of leverage. Economic dependence on credit and the high degree of system leverage are not a natural function of either capitalism or a free market. Instead, it is a system and phenomenon engineered by central banks. While the instability is not by design, the market structure very much is. Over the last four decades, central banks (including the Fed) have responded to every economic slowdown (or crisis) by increasing the money supply and reducing interest rates, such that existing debt levels could be sustained and more credit could be created. Each time the system as a whole attempted to deleverage, central banks worked to prevent it through monetary stimulus, ultimately kicking the can down the road and allowing decades of economic imbalance to accumulate in the credit system. This is the root cause of the inherent fragility within the financial system. And it is why each time an economic disruption surfaces, the monetary response from central banks needs to be larger and more extreme than before. With greater imbalance and more debt comes the need for even more QE to stem a liquidity crisis.

Each time, the entire system is pushed further and further out onto the same ledge. The terminal risk to the system (the stability of the underlying

currency) becomes greater and greater. Everyone is unwittingly forced to be along for this most unnerving of rides. This is the new normal, and there is nothing sustainable about it. But it is not a reality anyone must accept. There is a better way. For those paying attention to the actual game being played, bitcoin is increasingly becoming the clearest path to opt out of this insanity.

An Instrument of Freedom

At a very basic level, quantitative easing is a forced debasement (or devaluation) of monetary savings. It distorts every pricing mechanism within an economy, and its intended goal is the expansion of credit. When history books are written of this pre-bitcoin era, the failure to understand the consequence of distorting global pricing mechanisms will be identified as the source of all other critically flawed assumptions in modern central banking doctrine. There is no escaping it. You can only hope to manage the fallout. But where don't-tread-on-me meets the come-and-take-it mentality, freedom-loving *Americans* of all the world and of all walks of life are beginning to say enough is enough. There has to be a better way because there always is.

That is core to the very idea of hope and the very nature of human ingenuity. It is an unwillingness to accept the new normal as a fait accompli. If quantitative easing can be simplified down to a debasement of monetary savings, bitcoin can be simplified down to the freedom to convert value into a form of currency that cannot be printed. In *The Road to Serfdom*, Hayek describes the function of money most aptly: "It would be much truer to say that money is one of the greatest instruments of freedom ever invented by man."⁸² As he goes on to further explain, it is money that ultimately affords people a range of choice through trade, which is far greater than otherwise imaginable. It does so by distributing knowledge through its pricing mechanism, the single most important market signal (in aggregate), which facilitates economic coordination and the allocation of resources. However,

82. Friedrich A. Hayek, *The Road to Serfdom*, condensed version (*Reader's Digest*, April 1945), 62.

as the freedoms afforded by one monetary medium become impaired, it should be no surprise that human ingenuity would find a way to route around and spawn a new creation that performs that same function more effectively. That is bitcoin, and there is no going back. The proverbial cat is out of the bag and the distribution of knowledge is naturally exponential.

The promise of bitcoin is a more stable monetary system. There are no promises as to its value on any given day. The only assurance it provides is that its supply is not subject to manipulation or systematic debasement by a central bank (or anyone else). There is the seemingly constant question as to whether bitcoin is a “safe haven” and more recently, why bitcoin has become correlated to the broader (collapsing) financial markets. The simple reality is that bitcoin is not a safe haven, at least not as commonly defined in the mainstream. It is not widely held enough to possibly be a safe haven. It remains nascent, and it is perfectly predictable that, at the onset of a global deleveraging event and dollar liquidity crisis, a liquid asset would be sold along with everything else. However, what remains true, despite the turbulent times, is that bitcoin is the antifragile competitor to the inherently fragile financial system. It is the solution to the dollar.

Maximally Accountable

In his book *Antifragile*, Nassim Taleb describes antifragility as a quality that is not just robust or resilient but, instead, the opposite of fragile. Antifragile systems actually gain strength and feed on volatility.⁸³ The recent volatility in bitcoin is likely just the beginning, but it really represents uninterrupted and unceasing price discovery. There are no circuit breakers in bitcoin, and there are no bailouts. It is a market devoid of moral hazard, with each participant maximally accountable. When the dust settles, what does not kill bitcoin only makes it stronger—and in a literal sense. It is surviving and thriving in the wild without any central coordination. It is not for the faint

83. Nassim N. Taleb, *Antifragile: Things That Gain from Disorder* (Random House, 2012).

of heart, but it is the land of the free and the home of the brave. When it survives, there will still only be 21 million bitcoin, and its very survival will reinforce its place in the world. With each monetary stimulus injected into the legacy financial system, bitcoin's core value function will become more apparent and more intuitive to more people. This will not just occur by chance either. It will be because of the stark contrast bitcoin provides. Even with its volatility, bitcoin is laying the foundation for a more stable monetary system.

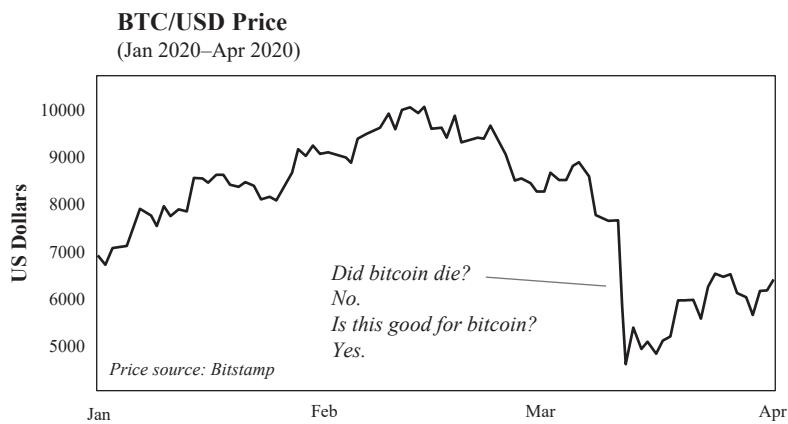


FIGURE 14.5
Price Source: Bitstamp

Because bitcoin's supply cannot be manipulated, its price and its supply of credit will similarly and forever be unmanipulable. Both will be determined on the market. As a result, the size of the bitcoin credit system will never sustain otherwise unsustainable imbalances. Beyond the nature of its fixed supply, this is where the contrast lies in practical application. The accumulation of sustained credit system imbalances (induced by central banks) is the inherent source of fragility in the global economy today. In a market built on the foundation of a currency that cannot be manipulated, as soon as imbalances arise, economic forces will naturally course-correct, preventing the system-wide and systemic credit risk that plagues the legacy financial

system. Rather than impair the future by allowing imbalances to accumulate beneath the surface, the unmanipulable supply of bitcoin will act as a governor to stamp out fires as soon as they appear. Fragile individual components of the system will be sacrificed, and the system as a whole will become more antifragile by that very same function.

For Joe Kernen, host of CNBC's *Squawk Box* (your modern-day average Joe), it was Facebook's Libra project that made bitcoin more intuitive. For others, it is hyperinflation in Venezuela. And now for many, it will increasingly become the incessant reality of recurring financial crises and QE. No matter how many cycles of QE the Fed and its global counterparts have in their bag of tricks, bitcoin is inevitably becoming a rallying cry for all those who see the impending train wreck and are unwilling to stand idly by. It is not just a collective act of civil disobedience. It is an individual recognition of the need to act in self-preservation. There comes a time for most everyone when common sense and survival instinct naturally take the reins. The avenue may be different for each individual, but at the end of the day, bitcoin is a means to preserve some form of freedom that is otherwise being impaired or infringed. Whether governments attempt to ban bitcoin or it is mistakenly blamed for the failures of the legacy system, always remember the simplicity of what bitcoin represents. It is nothing more than the individual freedom to convert real-world value into a form of money that cannot be manipulated. It is a most basic and fundamental freedom, but one that must be earned. So to all *Americans* in the world, stay humble, stack sats, and hold the damn line. Whatever it takes.



FIGURE 14.6

"The enemy has demanded a surrender. [...] I have answered the demand with a cannon shot."

—Lt. Colonel William B. Travis, February 1836⁸⁴

84. Travis, "To the People of Texas."

CHAPTER FIFTEEN

Bitcoin Is Common Sense

(Originally published on 1 May 2020)

Old Habits Die Hard

“Perhaps the sentiments contained in the following pages, are not yet sufficiently fashionable to procure them general favor; a long habit of not thinking a thing wrong, gives it a superficial appearance of being right, and raises at first a formidable outcry in defense of custom. But the tumult soon subsides. Time makes more converts than reason.”

—Thomas Paine, *Common Sense* (1776)⁸⁵

These were the opening remarks of Thomas Paine’s call for American independence in early 1776. At the time, a declaration of independence was far from a certainty, but in Paine’s view, there was no question. It wasn’t a debate. There was only one path forward. Still, he understood that public opinion had not yet caught up and naturally remained anchored to the status quo, with a preference for reconciliation rather than independence. Old habits die hard. Regardless of merit, the status quo tends to be defended, anchored in time to the way things have always been. However, truths have a way of becoming self-evident in time, more often due to common sense

85. Thomas Paine, *Common Sense* (Philadelphia, January 1776).

rather than any amount of reason or logic. One day, the truth is more likely to become painfully obvious through firsthand experience, which opens up a perspective that otherwise would not have existed, than it is from a textbook. While Paine was undoubtedly attempting to persuade an undecided populace with reason and logic, it was at the same time an appeal to not overthink what should already be self-evident based on lived experience.

In Paine's view, independence was not a modern-day IQ test, nor was its relevance confined to the American colonies. Instead, it was a common-sense test, and its interest was universal to "the cause of all mankind." In many ways, the same is true of bitcoin. It is not an IQ test. Bitcoin is common sense, and its implications are near-universal. Few people have ever stopped to question or understand the function of money. It facilitates practically every transaction anyone has ever made, yet no one really knows how or why. In short, the function of money is taken for granted, and as a result, it is a subject not widely taught or explored. Yet, despite a limited baseline of knowledge, there is often a visceral reaction to the idea of bitcoin as money. The default position is predictably to reject it. Bitcoin is an anathema to all notions of existing custom. On the surface, it is entirely inconsistent with what folks know money to be. For most, money is just money because it always has been. For any individual, the construction of money is anchored in time, and for most, it is very naturally not questioned.

But enter bitcoin, and suddenly everyone has a strong opinion on what is and isn't money. To the fly-by-night expert, it is certainly not bitcoin. Bitcoin is natively digital. It is not tied to any government or central bank. It is volatile and perceived to be "slow." It is not currently used en masse to facilitate direct commerce, and it is not inflationary. Just about every characteristic of bitcoin is inconsistent with what people associate with money. However, this is one of those rare instances where something that does not walk or quack like a duck is, in fact, a duck. And what you mistakenly thought was a duck was something entirely different all along. When it comes to modern money, *the long habit of not thinking a thing wrong, gives it a superficial appearance of being right.*

In its most recognized and accepted form, money is issued by a central bank. It is perceived to be relatively stable and is capable of near-infinite transaction throughput. It is widely used to facilitate day-to-day commerce, and the supply can be rapidly inflated to meet the “needs” of an ever-changing economy. Bitcoin presently has none of these traits, and as a result, it is most often dismissed as not meeting the standards of modern-day money. This is where overthinking a problem can cripple even the highest of IQs. Pattern recognition fails because the game has fundamentally changed. Most players just do not yet realize it.

Bitcoin is finitely scarce, it is highly divisible, and it is capable of being sent over a communication channel (and on a permissionless basis). There will only ever be 21 million bitcoin. Rocket scientists, brain surgeons and the most revered investors of our time could all respectively look at bitcoin and be confounded, not seeing its value. But at the same time, if posed with a straightforward question—would you rather be paid in a currency with a fixed supply that can’t be manipulated or in a currency that is subject to persistent, systemic, and significant debasement—an overwhelming majority of individuals would choose the former. All day, every day. And it wouldn’t be close.

“It’s probably rat poison squared.”

—Warren Buffett, May 2018⁸⁶

“Bitcoin—there’s even less you can do with it. [...] I’d rather have bananas. I can eat bananas.”

—Mark Cuban, September 2019⁸⁷

86. Warren Buffet, speech, Berkshire Hathaway Annual General Meeting, 5 May 2018.

87. Mark Cuban, “Mark Cuban Answers Business Questions from Twitter | Tech Support,” YouTube, *Wired*, 27 September 2019.

Money Doesn't Grow on Trees

As kids, we all learn that money doesn't grow on trees, but at a societal level or as a country, any remnant of common sense seems to have left the building. Just in the last two months, central banks in the United States, Europe, and Japan (the Fed, ECB, and BoJ) have collectively inflated the supply of their respective currencies by \$3.3 trillion in aggregate—an increase of over 20%.

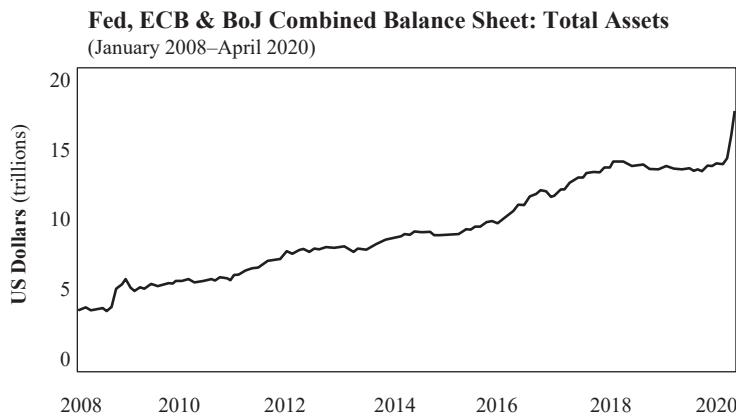


FIGURE 15.1
Source: Thomson Reuters Datastream

The Fed alone has accounted for the majority, minting \$2.5 trillion and increasing the base money supply by over 60% (see Figure 13.9). It's also far from over. Trillions more will be created. It is not just a possibility. It is a certainty. That deep feeling of uncertainty many are experiencing, the one that says "this doesn't make any sense" or "this can't end well"—that's common sense speaking. Few carry that thought process out to its logical conclusion, often because it is uncomfortable to think about, but the sense of unease is reverberating throughout the country and the world. While not everyone is connecting the dots between the mass amounts of money being created and bitcoin's fixed supply, a growing number are. Time makes more converts than reason. An individual doesn't have to understand how or why there

will only ever be 21 million bitcoin. All that must be recognized in practical experience is that dollars are going to be worth significantly less in the future, and then, the idea of a currency with a fixed supply naturally begins to make sense. In most cases, understanding exactly how bitcoin achieves its fixed supply comes after making the initial connection that the two are related. But even then, no one really needs to understand how bitcoin enforces its fixed supply to have an appreciation that a currency with a fixed supply would be valuable.

Michael Goldstein @bitstein

If people can print money, they will print money.

15 Sep 2018



FIGURE 15.2

For each individual, there is a choice to either live in a world where some people get to produce new units of money for free (but just not you) or a world where no one gets to do that (including you). From an individual perspective, the difference is not marginal. It is night and day. And anyone conscious of the decision intuitively opts for the latter, recognizing that the former is neither sustainable nor to their advantage. Imagine there were one hundred individuals in an economy, each with different skills. All have determined to use a common form of money to facilitate trade in exchange for goods and services produced by others. With the one exception that a single individual among them has the superpower to print money, requiring no investment of time and at practically no cost.

Given that human time is both an inherently scarce resource and a necessary input in the production of any good or service demanded in trade, such a scenario would functionally mean that one person would get to purchase the output of all the others for free. Why would anyone agree to such an arrangement? In the real world, this individual is a central bank. The perception

that a central bank is expected to act in the public's interest does not change the fundamental operation or its consequence. If it does not make sense on a micro level, it does not magically transform into a different fundamental fact merely by introducing greater degrees of separation and opacity. If no individual would bestow that power in another person, then it follows that no one would consciously decide to bestow it in a central bank.

Everything beyond this fundamental reality strays into abstract theory, relying on leaps of faith, hypotheticals, and big words that no one understands. It is not that one individual or central bank is more trustworthy than another, but simply that no individual is advantaged by someone else having the ability to print money (regardless of identity or interests). This leaves only one alternative: each individual would be advantaged by ensuring that no other individual or entity possesses this power. The Fed may have the ability to create dollars at zero cost, but *money still doesn't grow on trees*. It is more likely that a particular form of money is not actually money than it is that money has miraculously started growing on trees. While there is a long habit of not thinking this particular thing wrong, the errant defense of custom can only stray so far. Time converts everyone back into reality. At present, it is the Fed's "shock and awe" money-printing campaign contrasted by the simplicity of bitcoin's fixed supply of 21 million. And there is no amount of reason that can replace an observed divergence in two distinct paths.

Defending Existing Custom

"There's money and there's credit. The only thing that matters is spending and you can spend money and you can spend credit. And when credit goes down, you better put money into the system so you can have the same level of spending. That's what they did through the financial system and that thing worked."

—Ray Dalio, September 2017⁸⁸

⁸⁸ Ray Dalio, "Bridgewater founder Ray Dalio: We Have Two Economies Now," interview by Joe Kernan, *CNBC Squawk Box*, 19 September 2017.

As more people become aware of the Fed's activities, it only raises more questions. Think about it for a second. Two point five trillion—\$2,500,000,000,000—is a big number. Who gets the money, and why? What will the effects be? And when? Why is this even possible? All valid questions, but none change the fact that more dollars now exist and each will be worth materially less in the future. That is intuitive. However, at an even more fundamental level, recognize that the operation of printing money (or creating digital dollars) does nothing to generate economic activity. Imagine a printing press running on a loop, or simply keying in a number of dollars on a computer (which is technically all that the Fed does when it creates “money”). Such an operation does not produce anything of value in the real world. Instead, that action can only induce an individual to take some other action.

Recognize that any tangible good or service in existence must be produced by some individual or a group of individuals. Human time is the input. Capital production is the output. Whether software applications, manufacturing equipment, a service, or an end consumer good, one or more individuals had to contribute time to produce it. That time and value is what money tracks and prices, and ultimately what is traded and exchanged in return for money. Entering a large number into the computer does not produce software, hardware, cars, or homes. People produce those things, and money coordinates the preferences of all individuals within an economy, compensating value to varying degrees for time spent.

When the Fed creates \$2.5 trillion in a matter of weeks, it is consolidating the power to price and value human time in the Fed's hands. This, however, is not a suggestion that the individuals at the Fed are consciously or deliberately operating maliciously. It is just the inevitable consequence of the Fed's actions, regardless of how well-intentioned. Again, the Fed's operation (arbitrarily adding zeros to various bank account balances) cannot create value. All it can do is determine how to allocate new dollars. Doing so advantages some individuals, enterprises, or segments of the economy over others. In creating and allocating new dollars, the Fed replaces a market function—and one priced by billions of

people—with a centralized function, greatly influencing the balance of power as to who controls the monetary capital that coordinates economic activity. Think about the distribution of money as the balance of control influencing and determining what gets built, by whom, and at what price. At the moment of creation, more money exists but there is no more human time or goods and services available as a consequence of that action. Beyond the point of creation, the Fed's actions similarly do not, and cannot, create more jobs as a function of time or over time. There are just more dollars to distribute across the same labor force, but with a different distribution of those holding the currency. The Fed can print money (or create digital dollars), but it can't print time, nor can it do anything but artificially manipulate the allocation of resources within an economy.

No Free Lunches, Just More Dollars

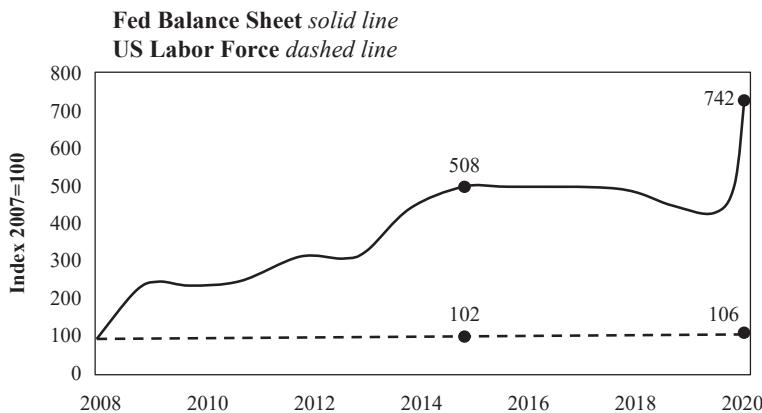


FIGURE 15.3

Sources: Federal Reserve Economic Data (FRED), US Bureau of Labor Statistics

Since 2007, the Fed balance sheet has increased over seven-fold, but the labor force has only increased by 6%. There are roughly the same number of people contributing output (human time) but far more dollars available to compensate for that time. Do not be confused by the impossible-to-quantify calculation

around a job saved versus a job lost. This is the US labor force, defined by the Bureau of Labor Statistics as all persons sixteen years of age and older, both employed and unemployed. The inevitable result is that the value of each dollar declines, but it does not create more workers. And prices do not all uniformly adjust to the increase in the money supply, including the price of labor.

In a theoretical world, if the Fed were to distribute the newly created money to individuals in equal proportion to the amount of currency previously held, the balance of power would not shift. In practice, the distribution of money is uneven, and the power shift is dramatic. The holders of financial assets (which the Fed purchases in the process of creating new dollars) and those with access to cheap credit (the government, large corporations, high-net-worth individuals, etc.) are heavily favored. In aggregate, the purchasing power of every dollar declines, just not immediately, and a small subset benefits at the cost of the whole (a phenomenon known as the Cantillon effect).



Method: calculating the change in different sources supplying reserves from these two reports.

FIGURE 15.4

Source: Federal Reserve System (US), H.4.1 reports dated 27 Feb 2020 and 30 Apr 2020.

Despite the consequences, the Fed takes these actions in an attempt to support a credit system that would otherwise collapse without an ever-increasing supply of dollars. In the Fed's economy, the credit system is the

price-setting mechanism because the amount of dollar-denominated debt far outstrips the supply of dollars, which is also why the purchasing power of each dollar does not immediately respond to an increase in the money supply. Instead, the effects of increasing the money supply are transmitted, over time, through an expansion of the credit system.

US Credit System Leverage Dynamics After New Dollars Added

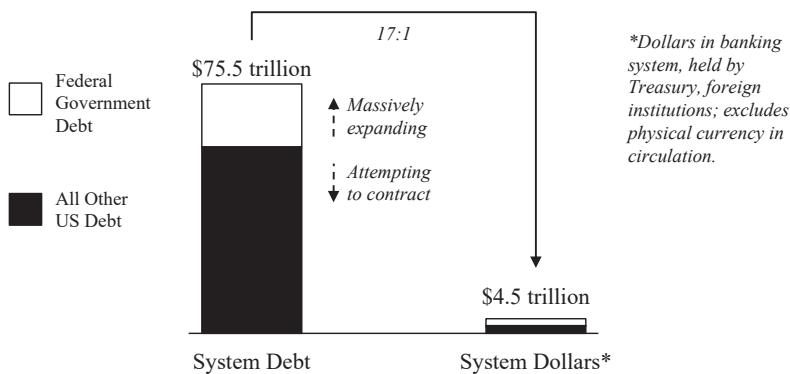


FIGURE 15.5

Source: Board of Governors, Federal Reserve (US); data as of original publication (May 2020).

When the credit system attempts to contract, it represents the market and the individuals within an economy working to eliminate imbalances that exist. By flooding the market with dollars, the Fed prevents what otherwise would be the natural course. It overrides the market's price-setting function and in doing so, fundamentally alters the structure of the economy. The market solution to the problem of too much debt is to reduce debt, while the Fed's solution is to increase the supply of dollars such that existing debt levels can be sustained. The goal is to first stabilize the credit system such that it can then expand further. The 2008 financial crisis provides a historical roadmap. In its immediate aftermath, the Fed created \$1.3 trillion new dollars in a matter of months. Despite this, the dollar initially strengthened as deflationary pressures in the credit system overwhelmed

the increase in the money supply. However, as the credit system began to expand, the dollar's purchasing power soon resumed its gradual decline. Currently, the cause and effect of the Fed's monetary stimulus is primarily transmitted through the credit system. It was the case in the years following the 2008 crisis, and it will hold true this time, provided the credit system remains intact.

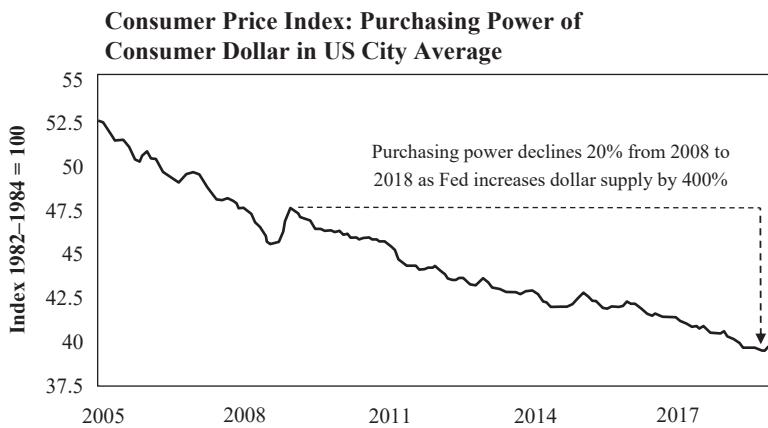


FIGURE 15.6
Source: US Bureau of Labor Statistics

How the effects manifest in the real economy is complicated, but it does not take any sophistication to recognize the general trajectory or to identify the foundational flaws. More dollars result in each dollar becoming worth less. And the value of any good—including monetary goods—naturally trends toward its cost to produce. The marginal cost for the Fed to produce a dollar is zero. However, all the bailouts from both the Fed and Congress, whether to individuals or companies, are ultimately paid for by someone. It is axiomatic that *printing money (or creating digital dollars) does nothing to generate economic activity*. It only shifts the balance of power as to who allocates the money and prices risk. It strips power from the people and centralizes it to the government. It also fundamentally impairs the economy's function by distorting prices everywhere. But most seriously, it

puts the stability of the underlying currency at risk, which is a cost everyone collectively pays. The Fed may be able to create dollars for free, and the Treasury may be able to borrow at near-zero interest rates as a direct result, but there is still no such thing as a free lunch. Someone still has to do the work, and all printing money does is shift who has the dollars to coordinate and price that work.

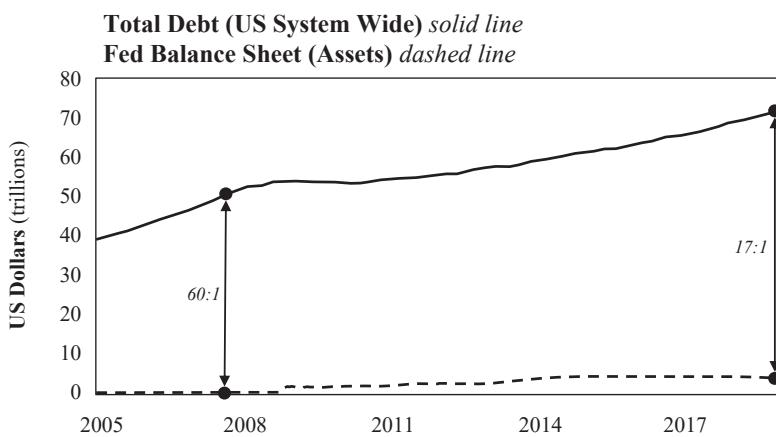
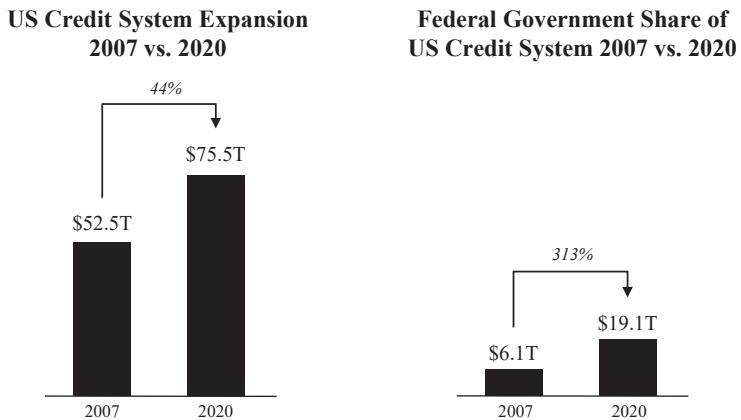


FIGURE 15.7
Source: Federal Reserve Economic Data (FRED)

The stamping of paper is an operation so much easier than the laying of taxes, that a government, in the practice of paper emissions, would rarely fail in any such emergency to indulge itself too far, in the employment of that resource, to avoid as much as possible one less auspicious to present popularity. If it should not even be carried so far as to be rendered an absolute bubble, it would at least be likely to be extended to a degree, which would occasion an inflated and artificial state of things incompatible with the regular and prosperous course of the political economy.

—Alexander Hamilton (first Treasury Secretary of the US)⁸⁹

89. Alexander Hamilton, *Final Version of the Second Report on the Further Provision Necessary for Establishing Public Credit (Report on a National Bank)*, US Department of Treasury, 13 December 1790.

**FIGURE 15.8**

Source: Board of Governors, Federal Reserve System (US), Z.1 Financial Accounts of the US

“Gospodin,” he said presently, “you used an odd word earlier—odd to me, I mean...”

“Oh, tanstaaf. Means there ain’t no such thing as a free lunch. And isn’t,” I added, pointing to a FREE LUNCH sign across room, “or these drinks would cost half as much. Was reminding her that anything free costs twice as much in long run or turns out worthless.”

“An interesting philosophy.”

“Not philosophy, fact. One way or other, what you get, you pay for.”

—from *The Moon is a Harsh Mistress*⁹⁰

Bitcoin Is Common Sense

Among its perceived flaws as a currency, critics view bitcoin as being too complicated to ever achieve widespread adoption. In reality, the dollar is complicated. Bitcoin is not. There will only ever be 21 million bitcoin and

90. Robert Heinlein, *The Moon is a Harsh Mistress* (G. P. Putnam’s Sons, 1966).

no one controls the supply of the currency. Not the Fed, not a CEO, not a company, not a government, not anyone. Bitcoin becomes very simple when understood through this lens. Bitcoin may be complicated at a technical level. It involves higher-level mathematics and cryptography, relies on a “mining” process, and contains several unfamiliar concepts like blocks, nodes, keys, elliptic curves, digital signatures, difficulty adjustments, hashes, nonces, and Merkle trees, among others. But with all this, bitcoin remains very simple.

If the supply of bitcoin remains fixed at 21 million, more people will demand it, and its purchasing power will increase. Nothing about the complexity under the hood will prevent adoption. Most participants in the dollar economy (even the most sophisticated) have no practical understanding of the dollar system at a technical level. The dollar system is not only far more complex than bitcoin. It is far less transparent. Similar degrees of complexity and many of the same primitives that exist in bitcoin underlie an iPhone. Yet, individuals manage to use the iPhone successfully without understanding how it works at a technical level. The same is true of bitcoin. The innovation in bitcoin is that it achieved finite digital scarcity while being easy to divide and transfer. Twenty-one million bitcoin, period. Compare this to \$2.5 trillion new dollars created by one central bank in just two months. Bitcoin’s fixed supply is the only common-sense feature anyone really needs to know.

A lot is happening in the background, but the supply of the currency drives everything. These are the dots that people worldwide are connecting. The Fed is creating trillions of dollars while bitcoin’s issuance rate continues to programmatically reduce by half approximately every four years. While most may not be aware of these two divergent paths, a growing number of people are (as knowledge distributes with time). But even a small number of people figuring it out creates a significant imbalance between the demand for bitcoin and its supply. When this happens, the value of bitcoin goes up. It is that simple and that is what draws everyone else in: price. Price is what communicates information. All those otherwise not participating react to

price signals. The underlying demand is ultimately dictated by fundamentals (even if speculation exists), but the majority do not need to understand those fundamentals to recognize that the market is sending a signal.

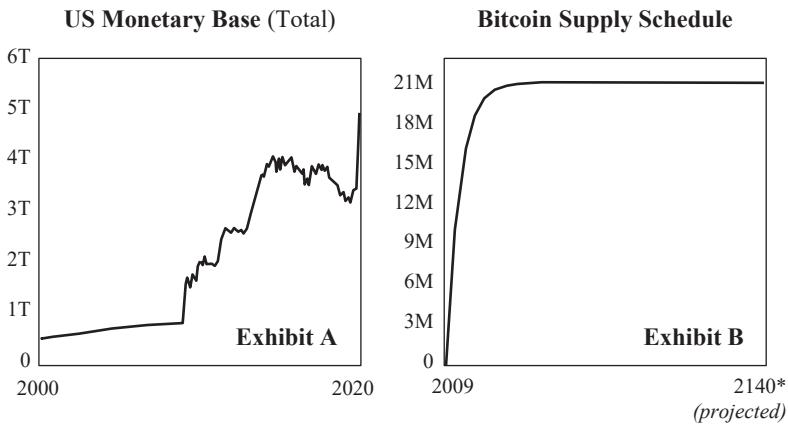


FIGURE 15.9
Source: Federal Reserve Economic Data (FRED)

Purchasing Power of Bitcoin Relative to Dollars: BTC/USD (Nov 2011–May 2020)



FIGURE 15.10
Source: Bitstamp

Once that signal is communicated, it then becomes clear that bitcoin really isn't that complicated. Download an app, link a bank account, and buy bitcoin. Get a piece of hardware, the hardware generates an address,

and you can send money to that address. No one can take it from you, and no one can print more. In that moment, bitcoin becomes far more intuitive. It seems complicated from the periphery, but anyone with common sense and something to lose will figure it out. The benefit is too great to ignore, and money is such a basic necessity that the bar (on a relative basis) only gets lower and lower in time. Self-preservation is the only motivation necessary to break down any remaining barriers.

A solid foundation underpins everything—bitcoin is a hard-capped money that cannot be counterfeited, is resistant to censorship and seizure, and can be secured without any counterparty risk. With that bedrock, it does not require a lot of imagination to see how bitcoin evolves from a volatile novelty into a stable currency facilitating day-to-day commerce. The contrast to the dollar is stark—a currency that becomes exponentially more expensive to produce over time versus a currency whose cost to produce is anchored forever at zero by its very nature. At the end of the day, bitcoin is a currency whose supply (and derivatively its price system) cannot be manipulated. Fundamental demand for bitcoin begins and ends at this singular cross-section. One by one, people wake up and recognize the distinction.

With bitcoin as a backdrop, it becomes self-evident that there is no advantage in ceding the power to print money or allowing a central bank to allocate resources within an economy in place of the individuals who comprise it. As each individual figures this out, bitcoin adoption grows. And as a function of that adoption, bitcoin will transition from volatile, clunky, and novel to stable, seamless, and ubiquitous. The entire transition will be dictated by value, and value is derived from the foundation that there will only ever be 21 million bitcoin. It is impossible to predict exactly how bitcoin will evolve because most of the minds that will contribute to that future have yet to comprehend it. As bitcoin captures more mindshare, its capabilities will expand exponentially beyond the span of resources that currently exist, but those resources will also come at the direct expense of the legacy system. It is ultimately a competition between two monetary systems, and the paths could not be more divergent.

Bananas grow on trees. Money does not, and there still ain't no such thing as a free lunch. Someone is paying for everything. When governments and central banks can no longer create money out of thin air, it will become crystal clear that backdoor monetary inflation was always just a ruse to allocate resources for which no one was actually willing to be taxed. There may be debate, but bitcoin is common sense. *Time makes more converts than reason.*

These proceedings may at first seem strange and difficult, but like all other steps which we have already passed over, will in a little time become familiar and agreeable: and until an independence is declared, the Continent will feel itself like a man who continues putting off some unpleasant business from day to day, yet knows it must be done, hates to set about it, wishes it over, and is continually haunted with the thoughts of its necessity.

—Thomas Paine, *Common Sense* (1776)⁹¹

91. Paine, *Common Sense*.

CHAPTER SIXTEEN

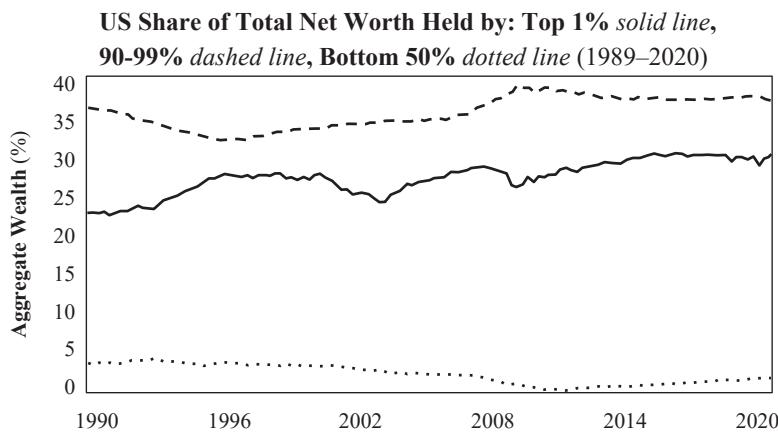
Bitcoin Is One for All

(Originally published on 27 August 2020)

Non-Political Solutions

At the 2020 Democratic National Convention, Congresswoman Alexandria Ocasio-Cortez described the Bernie Sanders presidential campaign as “a movement that realizes the unsustainable brutality of an economy that rewards explosive inequalities of wealth for the few at the expense of long-term stability for the many.”⁹² That the current economic system is working very well for a few at the expense of the many has become more widely recognized and accepted across both sides of the political aisle in recent years. While there is vehement disagreement on the appropriate solution, most everyone at least agrees that there is a problem. Fortunately or unfortunately, there is no political solution to a problem that is inherently economic in nature. It is unfortunate because politicians of all ideologies will make promises of grandeur while further dividing the nation in search of a political solution that does not exist. At the same time, it is fortunate that the answer is not political, as bridging partisan divides has historically proven to be a fool’s errand.

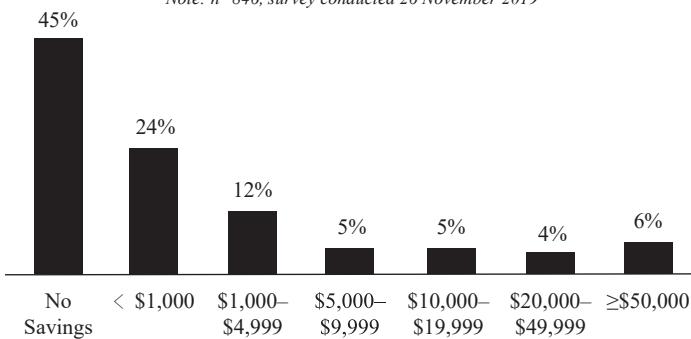
92. Rep. Alexandria Ocasio-Cortez, speech, Democratic National Convention, 18 August 2020, Milwaukee, WI.

**FIGURE 16.1**

Source: Federal Reserve Economic Data (FRED)

US Savings Accounts by Size (US\$)

Note: n=846, survey conducted 26 November 2019

**FIGURE 16.2**

Source: statista.com

The economic structure is, without a doubt, broken. Wealth gaps are only widening, and economic instability is everywhere. It's a reality that is hard to deny. The stock market and national average home values are back at all-time highs while tens of millions of Americans are filing for unemployment and half of society has practically no savings. It is suffocating many, and it applies globally. Politicians are simply not the answer. The fundamental problem with the current economic structure lies not in politics but in

the currencies that coordinate economic activity (e.g., the dollar, euro, yen, peso, bolivar, etc.), and no politician can fix problems that stem from the structural flaws inherent to modern money.

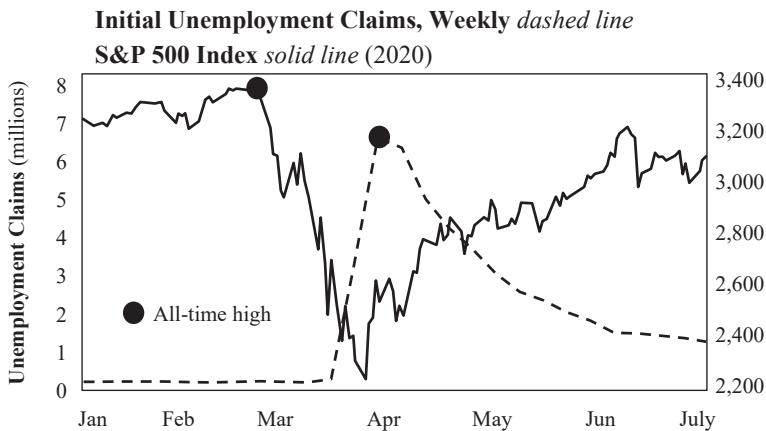


FIGURE 16.3

Sources: US Employment and Training Administration, S&P Dow Jones Indices

A currency is the foundation of an economy because it coordinates all economic activity via trade. If an economy is functionally breaking down, it would be more appropriate to say that the underlying currency is not effectively coordinating economic activity. The currency is the input, and the economy is the output. In short, the fly in the ointment is the money. While many are focused on how to address massive wealth inequality, very few make the connection to the money everyone is using as the source of the problem. It's not just that the economy is not working for many. The dollar as the primary mechanism for coordinating economic resources is failing everyone. Economic imbalance is the new normal, but nothing is normal about sustained imbalance. In fact, it is an economic oxymoron. Balance is critical to the functioning of any economy, and when functioning properly, an economy would naturally eliminate imbalance in its normal course. An economy that actively sustains imbalance, rather than eliminating it, is evidence itself of a broken economic structure. While the massive and growing

economic imbalance that exists today is often believed to be endemic to capitalism, it is principally a result of central bank monetary policy and the failure of the dollar.



FIGURE 16.4

Portrait of Bitcoin Sign Guy during Janet Yellen's Testimony
(House Financial Services Committee Hearing on 12 July 2017) by Jim Ferguson, 2020

Central bank monetary policy is the exogenous force creating economic distortion and extreme levels of inequality. The mere existence of economic inequality is not in itself an inequity. In fact, unequal outcomes are both natural and entirely consistent with economic balance. However, the inequality created and exacerbated by a flawed monetary system *is* an inequity. It is unnatural and exogenous to a free-market economy. The structural flaw inherent to the dollar currency system (or any fiat currency system) is the force most responsible for the sustained economic imbalance. Unsustainable and extreme wealth disparity follows from that imbalance. Every other distortive economic action or policy is secondary to the manipulation of the money itself. That is the root of all structural economic problems, and until it is fixed, the world will remain suspended in an increasingly fragile state. The legacy monetary system centralizes and consolidates wealth, which is the output of sustaining and exacerbating economic imbalance. It is a system that works for a few in the short term yet fails everyone in the long term. As imbalances grow, the currency's ability to coordinate economic activity

degrades gradually and eventually fails completely. When a currency fails, everyone pays the price—even those who initially benefited the most.

Bitcoin is the polar opposite. It is one currency that works for all, now and in the future. It eliminates imbalance as a natural function, wherever and whenever it appears, because its supply cannot be manipulated. With a fixed supply capped at 21 million and ever-increasing adoption, bitcoin is owned by more and more people as time passes, with each controlling a smaller and smaller share of the same fixed pie. The ownership of the currency naturally becomes more distributed and less concentrated over time, which provides the foundation for greater balance. Bitcoin levels the playing field and ensures that the monetary system cannot itself be a source of extreme inequity. It does so by guaranteeing certain inalienable rights. Every currency holder is assured that more units of the currency will not be arbitrarily produced, and each currency unit is treated equally within the network. Bitcoin coordinates economic activity more effectively because its pricing mechanism cannot be distorted or manipulated by exogenous forces, which is the fatal flaw of the legacy currency system. A fixed supply, equal protection, and true price signals deliver greater balance. Bitcoin fixes the economic foundation for everyone such that everything else can then begin to repair itself.

The Role of Money and the Price System

Think about money as the coordination function within an economy, where the utility of money is to intermediate a series of exchanges. Receive, hold, spend. It's that simple.⁹³ Money is the intermediary good used to both quantify and trade value. As the market converges on a common form of money, a price system emerges, allowing the subjective concept of value to be more objectively measured. Money is the pricing mechanism, and the output is a pricing system. The price system communicates information. It aggregates

93. Credit to Pierre Rochard for this distillation.

individual preferences within an economy and communicates those preferences through local prices, as measured in a common monetary medium. Every time a good or service is priced and bought, that is a communication of preference. Change in prices reflects changes in preferences. And because preferences are ever-changing, so too are prices.

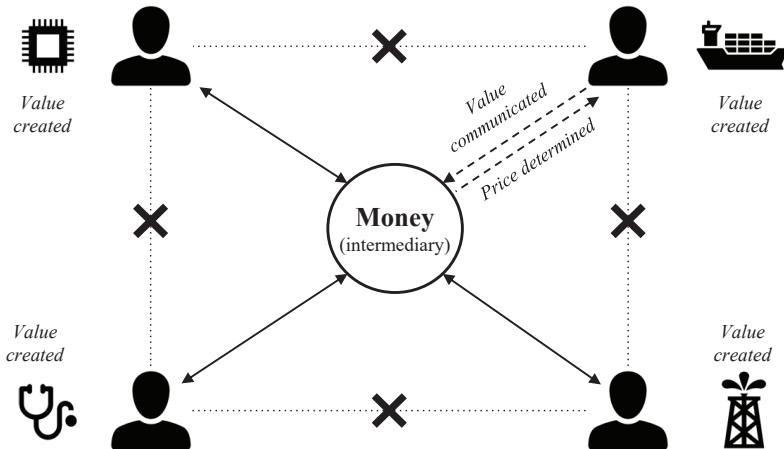


FIGURE 16.5

There are millions of goods within a developed economy, each with individual prices resulting in billions of relative price signals. Relative price signals ultimately communicate exchange ratios between various combinations of goods. While the value of any single good may be static for a period of time, certain prices are always changing within an economy, which dictates that relative prices are ever-changing. An economy constantly works to find balance through the aggregate changes in price levels. Every change, up or down, is an attempt to find balance and eliminate imbalance through trial and error. Everyone within an economy reacts to the price signals most relevant to their own preferences, which naturally change and become dynamically influenced by changing prices themselves. Through the price system, individual market participants learn what others value and what they need to produce to meet their own needs. As prices change, behaviors

change, and everyone adapts. The price system is the *visible* hand that allows for balance to be achieved and for imbalance to be identified and eliminated. Long-term economic stability is achieved because variable information is constantly communicated through the price system. It is the fluctuation in prices, when not distorted, that actively prevents large-scale and systemic imbalances from forming.

Flaws of the Central Bank Mandate

Most central banks, including the Fed, have the authority to create money arbitrarily at no cost and have a mandate to maintain stable prices (i.e., a price stability mandate). This combination is fatal to the functioning of any price mechanism and ultimately to the underlying economy. When a central bank targets the stability of any price level, it works against the natural course of an economy, which seeks to find balance and adapt to changes in preferences through the price system. In the pursuit of price stability, central banks manipulate the money supply, distorting every price in the world. With each exogenous attempt to achieve price stability, existing imbalance is sustained and bad information is distributed to every person within the economy through false price signals, ensuring more imbalance accumulates. Imagine this happening each time the economy tries to find balance. By sustaining imbalance, those who benefit from its existence are advantaged at the expense of everyone else.

This process also impedes the ability of those on the lower end of the economic spectrum to contribute and to command a greater share of the resources within an economy. While increases and decreases to the money supply both distort economic activity, central banks increase the money supply over time, which has the effect of artificially maintaining higher price levels than would otherwise be sustained. Artificially inflated prices create an uphill battle for those who have little savings and do not own assets. Inflated asset prices become further out of reach for those who do not own them, and higher prices of goods financially squeeze those with the least

savings the most. False price signals also induce poor economic decisions, disproportionately harming those on the lower end of the economic spectrum who can least afford errors and setbacks. While the manipulation of the money supply is counterproductive to everyone in the long run, there are winners and losers in the short term. The rich get richer and the poor get poorer.

As a tangible example, during the 2008 financial crisis, the value of real estate was declining. The economy's price mechanism was communicating that an imbalance existed in the value of real estate. In aggregate, market participants were communicating an increasing demand for money relative to a decreasing demand to hold real estate. At that particular moment in time, the actual amount of money and the available supply of real estate were not rapidly or meaningfully changing. Instead, preferences within the economy were shifting, as were relative price signals. Rather than allow the economy to find balance and eliminate imbalance, the Fed increased the supply of dollars to "stabilize" the dollar value of real estate. More literally, it created \$1.7 trillion to purchase mortgage-backed securities as a direct means to prop up the value of real estate, particularly the housing market. Those that owned real estate or operated businesses dealing in the production (or financing) of real estate benefited disproportionately, and at the direct expense of those that did not. Imagine someone saving to buy a home. Just as prices were coming down, which would have made a home more affordable, the Fed stepped in to increase the price of real estate, specifically housing, making it that much more expensive and further out of reach. The marginal benefit skewed to those who "had" at the expense of those who "had not," just as it always does when imbalance is sustained.

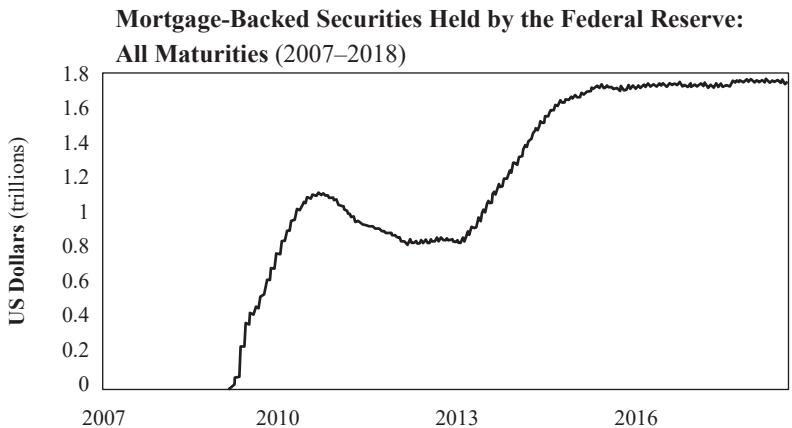


FIGURE 16.6
Source: Federal Reserve Economic Data (FRED)

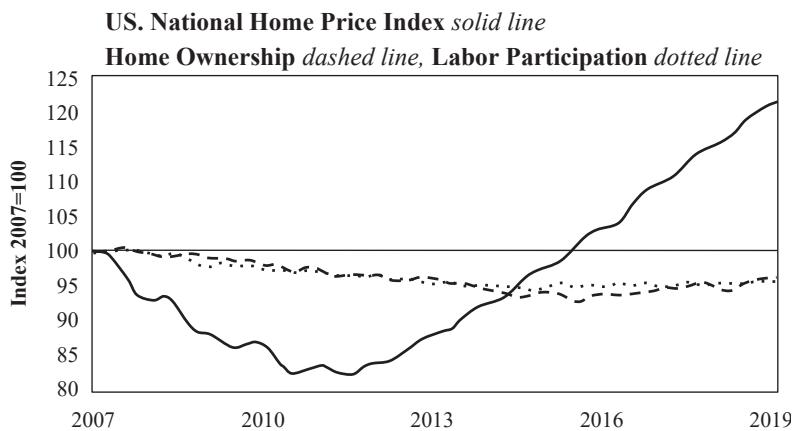


FIGURE 16.7
Sources: FHFA National Home Price Index, US Bureau of Labor Statistics

The Fed actively manipulated the value of real estate, but it also distorted all price signals within the economy by significantly increasing the money supply. The natural market function would have seen prices adjust to eliminate imbalance. But the Fed's solution was the opposite. It devalued the money (by increasing its supply) such that the value of real estate (among other goods) as priced in dollars would change the least. Rather

than eliminate imbalance, the Fed's actions allowed imbalances to be sustained and actually grow. Sustaining imbalance is precisely what occurs each time the Fed intervenes to stabilize price levels. However, stability when achieved through manipulation merely suppresses volatility. It creates an unnatural rigidity in price when price fluctuation is both a desired state and the natural function of a market communicating changes in preferences to find balance. When imbalances that would otherwise be eliminated are allowed to be sustained through artificial means and for extended periods of time, it ultimately creates greater volatility in the long run and critically impairs the ability of a monetary medium to coordinate economic activity, which is its singular utility. Each time and cumulatively, it advantages and further embeds the incumbents, just as the market is working to eliminate imbalance.

Rather than have a billion people who actually make up an economy set prices, a few people unilaterally change the whole game by clicking some buttons on a computer screen; it distorts the entire value chain of the pricing mechanism.

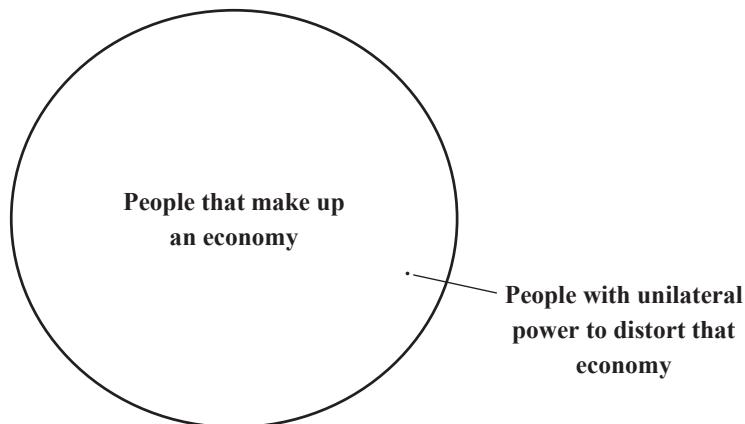


FIGURE 16.8

By manipulating price levels, the Fed isn't just preventing smaller intermittent fires from naturally running their course. The accumulation of imbalances causes larger fires down the road. Think of the Fed as the arsonist that lights

a fire, leaves through the back door in the middle of the night, and is then celebrated as the hero when it arrives through the front door to fight the fire with gasoline. A change in price levels, even if particularly volatile, is not a fire that needs putting out. Artificially preventing changes in price (i.e., a price stability mandate) is what lights the fire in the first place. The Fed co-opts the entire value chain of the pricing mechanism. Change in price is actually desired and the central bank works in opposition to that change by manipulating the money supply. The formation of imbalance within an economy is natural. Creating a centralized mechanism that prevents imbalances from being eliminated is the unnatural and damaging part. It also creates long-term economic instability by distorting price signals over decades and widens the wealth gap by constantly advantaging those on the right side of the imbalances. Predictably and unironically, the existence of the central bank's price stability mandate, combined with the power to print money, causes both long-term instability and sustained economic imbalances—exactly as Hayek forewarned.

In fact, in the case discussed, the very measures which the dominant “macro-economic” theory has recommended as a remedy for unemployment, namely the increase of aggregate demand, have become a cause of a very extensive misallocation of resources which is likely to make later large-scale unemployment inevitable. The continuous injection of additional amounts of money at points of the economic system where it creates a temporary demand which must cease when the increase of the quantity of money stops or slows down, together with the expectation of a continuing rise of prices, draws labour and other resources into employments which can last only so long as the increase of the quantity of money continues at the same rate—or perhaps even only so long as it continues to accelerate at a given rate. What this policy has produced is not so much a level of employment that could not have been brought about in other ways, as a distribution of employment which cannot be indefinitely maintained and which after some time can be maintained only by a rate of inflation which would rapidly lead to a disorganisation of all economic activity. The fact is that by a

mistaken theoretical view we have been led into a precarious position in which we cannot prevent substantial unemployment from re-appearing; not because, as this view is sometimes misrepresented, this unemployment is deliberately brought about as a means to combat inflation, but because it is now bound to occur as a deeply regrettable but inescapable consequence of the mistaken policies of the past as soon as inflation ceases to accelerate.

—Friedrich A. Hayek⁹⁴

Most mainstream economics professors readily agree that price-fixing or setting quotas on certain economic goods naturally creates economic inefficiency and imbalance. However, the same experts then turn around and avidly defend central bank monetary policy, ignoring the fundamental inconsistency. Economic manipulation is economic manipulation. Rigidity in the price or quantity of any economic good driven by exogenous forces results in imbalance. Variance allows for balance and equilibrium. It is a logical and uncontroversial view. Why then is the same principle not understood when applied to money? Imbalances are created when central banks target interest rates by manipulating the money supply, just as imbalances are created when the Venezuelan government arbitrarily sets the price of a gallon of gas below its market value. Ironically, manipulating the money supply happens to be economically more destructive because it distorts *all* prices within an economy, including relative price signals (as individual price levels do not adjust proportionately). When the Fed pursues its price stability mandate, it actively sends false price signals throughout an economy, causing imbalances in supply and demand structures to be sustained. Price stability is price manipulation. Predictably, manipulating the price of money to achieve any definition of stability causes a degree of economic distortion far worse than the manipulation of any single market.

⁹⁴. Friedrich A. Hayek, “The Pretense of Knowledge,” Lecture in the Memory of Alfred Nobel, 11 December 1974, Stockholm, Sweden.

We must look at the price system as such a mechanism for communicating information if we want to understand its real function—a function which, of course, it fulfills less perfectly as prices grow more rigid. (Even when quoted prices have become quite rigid, however, the forces which would operate through changes in price still operate to a considerable extent through changes in the other terms of the contract.) The most significant fact about this system is the economy of knowledge with which it operates, or how little the individual participants need to know in order to be able to take the right action. In abbreviated form, by a kind of symbol, only the most essential information is passed on, and passed on only to those concerned. It is more than a metaphor to describe the price system as a kind of machinery for registering change, or a system of telecommunications which enables individual producers to watch merely the movement of a few pointers, as an engineer might watch the hands of a few dials, in order to adjust their activities to changes of which they may never know more than is reflected in the price movement.

—Friedrich A. Hayek⁹⁵

Consequences of Sustaining Imbalance

The effects of sustaining imbalance can be best understood and observed through the credit system, which is where the Fed directly intervenes and consequently where the greatest distortion and imbalance exists. As the economy slows, the Fed increases the supply of dollars in the financial system by purchasing debt instruments (typically government treasuries) and crediting the sellers' accounts with newly created dollars. At the onset, the credit system was just a tool to effect monetary policy. It was the mechanism through which the Fed pursued its price stability mandate. The playbook was as follows. The Fed would increase the supply of dollars by purchasing credit instruments and reduce interest rates by the same mechanism. This

95. Friedrich A. Hayek, "The Use of Knowledge in Society," *American Economic Review* 35, no. 4 (September 1945): 526–527.

would induce economic expansion via cheap credit, and general price levels would stabilize. At least, that was the theory and intent.

US Credit System Leverage Dynamics After New Dollars Added

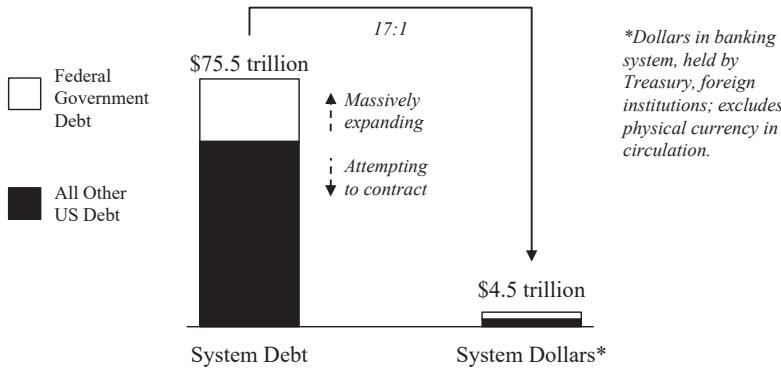


FIGURE 16.9

Source: Board of Governors, Federal Reserve System (US);
data as of the time of original publication (August 2020).

Now the tail is wagging the dog. Today, the credit system in the US stands at more than \$75 trillion systemwide, whereas there are only \$4.5 trillion actual dollars within the banking system. Approximately \$17 of dollar-denominated debt exists for every dollar (a debt-to-dollars ratio of 17:1). This degree of leverage is an economic imbalance, and it is only sustained as a function of the Fed. Each time the credit system attempts to contract, the Fed creates more dollars to help maintain the size of the credit system such that it can further expand. Because the credit system is now orders of magnitude larger than the base money supply, economic activity today is largely coordinated by the allocation and expansion of credit rather than by the base money itself. In aggregate, the credit system is the marginal price setter, given its size relative to the base money supply. The Fed's price stability mandate necessitates maintaining the size of the credit system, and in order to do so, the Fed must target asset prices that support existing debt levels. It has become circular. The Fed used the credit system as a tool to

stabilize price levels, but now, to maintain stable prices, it must maintain the size of the credit system.

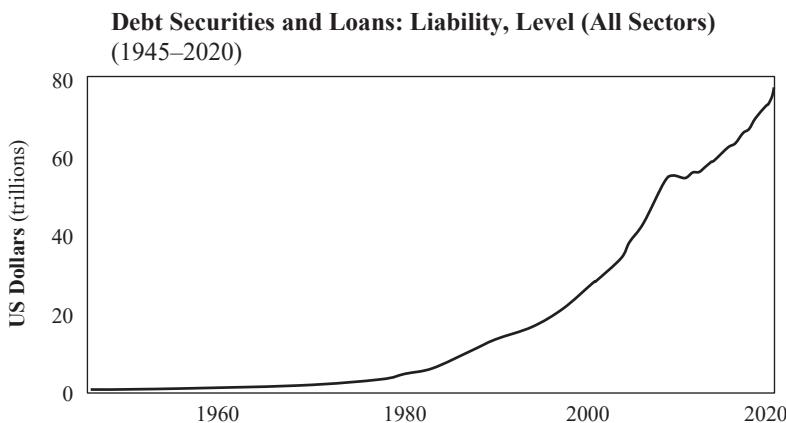


FIGURE 16.10
Source: Federal Reserve Economic Data (FRED)

This vicious cycle only exists because the Fed has unilateral control of the money supply, which was not always the case. In 1971, President Nixon officially ended all convertibility of dollars to gold,⁹⁶ and the US government later decoupled the dollar's value from gold altogether in 1976. The Fed's creation in 1913 and President Roosevelt's 1933 ban on the private ownership of gold might have set the stage,⁹⁷ but the complete departure from gold as a monetary anchor in the 1970s removed constraints that otherwise prevented the true centralization of the money supply. Ever since, the Fed has had unilateral control of the money supply, and the removal of these constraints paved the way for the Great Monetary Inflation, a phenomenon Paul Tudor Jones recently wrote about.⁹⁸ The sea change in the 1970s is what opened the door for the Fed to take a more central role in actively

96. Richard Nixon, public address to the nation, 15 August 1971.

97. Franklin D. Roosevelt, *Executive Order 6102—Forbidding the Hoarding of Gold Coin, Gold Bullion and Gold Certificates*, 5 April 1933.

98. Paul Tudor Jones and Lorenzo Giorgianni, “Market Outlook—Macro Perspective: The Great Monetary Inflation” (whitepaper, 9 May 2020).

managing the economy via the money supply. As a direct consequence, the base money supply and the credit system have expanded over the past five decades in ways that would otherwise not have been possible. Imbalances have been allowed to grow consistently over time, creating long-term economic distortions.

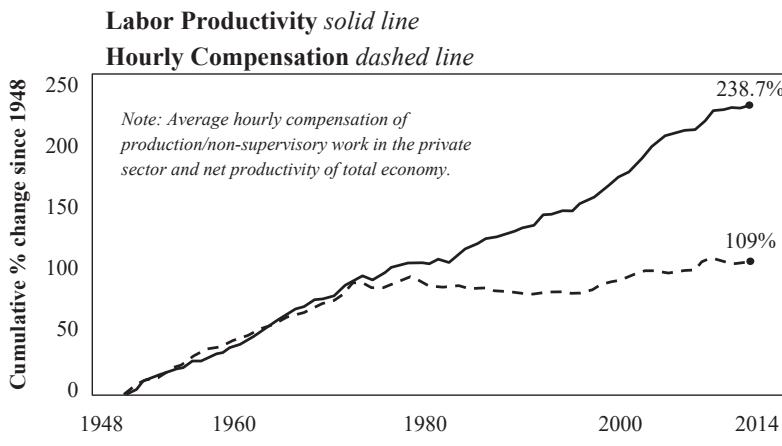


FIGURE 16.11
Source: Economic Policy Institute (data: US BEA, BLS)

When imbalances emerge in the credit system (i.e., too much debt relative to dollars), the Fed supplies more dollars such that existing debt levels can be sustained. Rather than write off bad debt and reduce existing debt levels, imbalances are actively sustained rather than eliminated. This is why the banking sector has become so large and the function of credit so central. It would not have been possible if the Fed could not print money to sustain otherwise unsustainable levels of debt, all in pursuit of “price stability.” Effectively, each time the banking sector would otherwise contract, the Fed undertakes measures to prevent it. It sounds crazy because it is. But the credit system exists the way it does because it is the primary transmission mechanism of the Fed’s monetary policy. The Fed needs the credit system to be maintained because it is through this vehicle that the Fed attempts to “manage” the economy. The Fed sees targeting asset prices to sustain debt

levels as less disruptive than allowing debt to be restructured and written off. From the perspective of the Fed, it's six one way, half a dozen the other. Effectively the same, but with less disruption. In reality, one path is economic manipulation of the worst kind, and the other is the natural and organic rebalancing of an economy in imbalance.

While it should be obvious that asset price targeting advantages those with assets (the wealthy) and is a regressive tax on those without assets (the poor), the Fed does have a price stability mandate. For those on the lower end of the economic spectrum with little to no savings, cash naturally represents most, if not all, of one's savings. Those at the higher end of the economic spectrum typically hold cash in addition to equity in businesses, real estate, and financial assets such as stocks and bonds. Again, consider the 2008 financial crisis. There were imbalances in the housing and financial markets. Prices were at unsustainable levels. As imbalance was in the process of being organically eliminated and price levels were correcting, the Fed stepped in to "stabilize" asset prices. Imagine if you had just entered this economy without any savings, a home, or stocks and bonds. Everyone who owned assets received a bailout at the expense of those who did not, all in the name of price stability.

Increasing the supply of dollars naturally causes the value of each dollar to decline. Wages (labor) paid in dollars were devalued, and asset prices were directly manipulated higher. Inflation of almost all consumer goods broadly followed. It is the equivalent of being hit from both sides for those lowest on the economic spectrum without assets and little savings. Wages purchase less with each passing day, and it becomes measurably more difficult to accumulate the amount of savings necessary to purchase assets. Initially, the effects are, at best, zero-sum. Those at the top benefit and those at the bottom suffer. In the end, everyone loses because the end game is economic instability. Notice the negative correlation below between housing prices and housing affordability (Figure 16.12), and then recognize that the Fed actively manipulates housing prices. Also recognize that housing prices are at an all-time high (above 2007 bubble levels) while nearly half the country

has no savings. This scenario can only exist in a manipulated world, and it crushes those without savings.

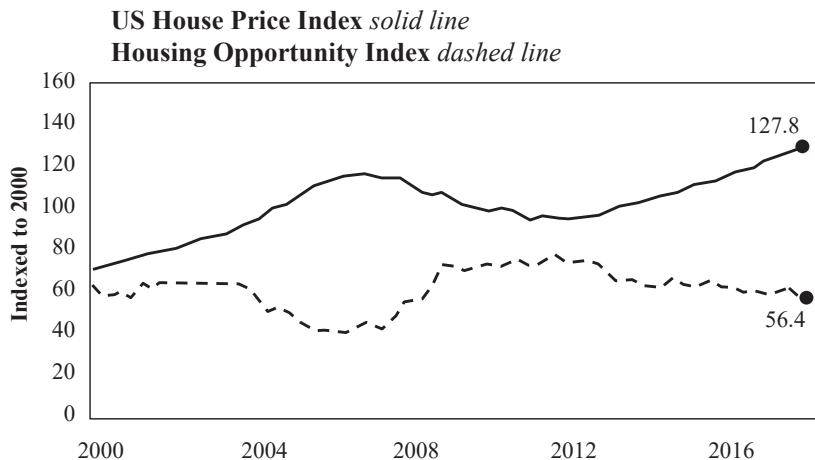


FIGURE 16.12

Source: Statista.com (data: US FHFA, National Association of Homebuilders)

The economists running the show and those who benefit the most will overwhelmingly agree it has to be done (every time). History is written by the winners, after all. But it is still all smoke and mirrors regardless of any proffered justification.

Sure, it was a crazy experiment, but the Fed had no other choice. Just imagine all those on the lower end of the spectrum that would have lost their jobs if not for the Fed's actions. Without a job, the poorest on the economic spectrum would have been far worse off and would not have been able to afford a home.

This is the common, predictable defense. The same line has certainly been used to defend the Fed's most recent actions in response to the global pandemic (printing \$3 trillion, with a T). While it may seem like logic, it lacks any fundamental economic argument in defense of the manipulation of price levels. The narrative is caught in a vicious cycle that begins with economic imbalance as a starting point (and one created by decades of the same distortive monetary policy). Recall the role of the arsonist hailed as a hero

fighting the fire. You cannot dig yourself out of a hole by continuing to dig in the same direction. At a fundamental level, manipulating price levels allows imbalances to be sustained that would otherwise course correct. It disproportionately advantages those that contributed to, and benefited the most from, the very existence of imbalance—like having your cake and eating it too, or like getting a second bite at the apple. Those who took an inadvisable risk get bailed out, rather than penalized, and the world of imbalance is sustained. The advantages gained from manipulated incentive structures are allowed to continue in a way that would not be possible absent the Fed's policy decisions.

An Unmanipulated Economic Structure

While there is never perfect balance, the existence and fluctuation of price levels are how an economy works toward balance through trial and error. Every individual reacts differently to an ever-changing set of price signals. It is how people evaluate which businesses to create, which skill sets to acquire, and which jobs to pursue. All of which are interdependent on each individual's interests, values, and capabilities. Imbalances can naturally arise within an economy as individuals speculate and overinvest in certain segments based on imperfect expectations of consumer preferences. That is the nature of trial and error. Nobody knows or can predict the future. Price signals are used to best guide decisions. A business or individual produces a good for x and attempts to sell it for y . If insufficient demand exists to make the activity profitable, that is the market communicating information to the producer. Better luck next time. Build something else or find another method that provides greater value (or is valued by more people). Imbalances are eliminated through this process. Those that take the risk own the consequences. It's a never-ending game that marries individual ideas and skills with the preferences of other market participants.

“Prices and profits are all that most producers need to be able to serve the needs of men they do not know. They are tools for searching—just as, for the soldier or hunter or seaman, the telescope extends the range of vision.”

—Friedrich A. Hayek⁹⁹

Money is the tool used to coordinate resources and to test the market by trial and error. It is the foundation of a price system that distributes information to all participants—the better the money, the more reliable the price system. And the more reliable a price system, the greater the balance in an economy. Those who deliver the greatest value to the largest number of people within an economy are naturally rewarded with the most money. But money would be of little value to the producer if others were not also producing goods that they themselves valued. The system would not sustain itself if balance did not exist. Purchasing a good or service from another individual requires that one must have first earned money. And providing goods valued by others is a far better outcome for everyone in aggregate than money being acquired through any other means (such as stealing or printing). It is the only way for the cycle of trade to be repeatable and symbiotic rather than one-off and zero-sum. What good is a customer that runs out of money or doesn’t have any in the first place? In a balanced economy, every producer is a customer of someone else and vice versa. As the old saying goes, “Give a man a fish, and you feed him for a day; teach him how to fish, and you feed him for a lifetime.”

One need not be religious to comprehend the wisdom. Everyone is incentivized to produce output valued by others within an economy, and each individual benefits from more people producing a wider range of goods or services. All participants have a selfish interest in delivering value to others and helping others contribute value in return. But this is not just a naive or hopeful economic view of the world. There are discernible benefits to trade,

99. Friedrich A. Hayek, *The Fatal Conceit: The Errors of Socialism* (University of Chicago Press, 1988), 104.

specialization, and a broader range of choices for all individuals. Money coordinates the division of labor, and the form of money with the most reliable pricing mechanism will consistently deliver the greatest value with the widest range of choice and balance. The pricing mechanism with the least distortion provides the clearest signals as to what others value and, derivatively, provides the greatest assurance that the information communicated is not a false signal. When free of manipulation, the function of a monetary medium and its price system naturally eliminates imbalance. It is the governor of the economic system that creates balance and enables symbiotic relationships to continuously be discovered through trial and error.

A Manipulated and Broken Economic Structure

The Fed's monetary policy actively prevents the economy from restructuring and finding balance. When imbalance exists, efforts to maintain price stability equate to maintaining otherwise false price signals. Productive assets remain in the hands of a few, and the world remains suspended in a state of imbalance. Money that does make its way to those on the lower end of the economic spectrum inevitably finds its way back to the owners of productive assets. The natural healing process is stymied each time the Fed intervenes as the economy cannot sustainably cycle money through trade in a symbiotic way. The skill sets and preferences of market participants remain out of sync. By pumping money into a structurally broken economy, the Fed is giving a man a fish while preventing him from learning how to fish. The existence of imbalance indicates that the composition of an economy is not meeting the needs of participants that make up the market. If the economy were allowed to restructure, the individuals and assets that capture an otherwise unsustainable share of wealth would not continue to do so.

When the Fed intervenes to keep the dream alive, it prevents the economy from rebalancing and creates inequity. Giving all benefit of the doubt, the Fed believes it is helping. It sees its activities as smoothing out market signals rather than manipulating them. The foundational assumption of the

Fed's economic theory is that active management of the money supply is a positive economic force. Active management of the money supply is in its DNA—it is a question of how much and when, not if. Would anyone expect the Fed to be an honest evaluator of its actions? It would be like grading your own test. No one would reasonably expect an objective assessment because there can be no objectivity. Certain false assumptions are encoded as true, which prevents the possibility of objectivity. The societal consequences have been disastrous, yet the Fed looks everywhere for answers, except in the mirror. And so it persists. The same policies are repeated over and over, always with the expectation of a different result.

Inequality is something that has been with us increasingly for more than four decades; it's not really related to monetary policy. It's more related to [stutter] there are a lot of theories on what causes it, but it's been something that's more or less been going up consistently for more than four decades, and there are a lot of different theories, one of which is just that globalization and technology call for rising levels of skills and aptitudes and education and that US educational attainment flattened out, certainly relative to our peers, over that period.

—Jerome Powell, chairman of the Federal Reserve, June 2020¹⁰⁰

Fed Chairman Powell recently provided this statement in response to a question about the Fed's contribution to increasing wealth inequality. Notice how the answer is not an argument for why central bank policy does not cause imbalance and inequality but more of a pronouncement followed by "look over there." Never believe the myths about globalization and technology driving wealth inequality. Nothing about technology, innovation, and globalization causes sustained economic imbalance or a structurally expanding wealth gap within an economy. For innovation to be valuable, it must, by definition, solve a problem for a range of people who can afford it. Value becomes

100. Jerome Powell, Press Conference, 10 June 2020.

self-referencing in that sense. Economic balance is a governing input to value. To believe the tall tales that technology and globalization cause economic imbalance, one would have to be willfully blind to the impact of centralizing the money supply. This centralization, in turn, caused banking to become the epicenter of the economy, making it possible for imbalance to be sustained as a policy decision over decades. There may be many theories, but the manipulation of every price signal within the economy is ground zero to economic imbalance and inequity. The structural flaw in the foundation creates the un-level playing field off of which all other contributing factors compound.

If A then B—if not A then not B

Money is the bedrock of economic systems. Understanding the fundamental and foundational role money plays in the economic engine establishes the logical connection between systemic economic issues of imbalance and the artificial manipulation of the money supply. Of course, there are other factors at play. The money supply is not the only way economic activity is manipulated. Tax policy, government spending, and the regulatory apparatus all contribute. However, focusing on these factors would be like trying to fix the windows on the hundredth floor of a building while a single Jenga block is supporting the foundation. That is the relationship between the issues inherent in the monetary system (the foundation) and all other economic issues (higher levels). The core problem that bitcoin solves is the foundation. If everyone displayed a little humility, each would recognize that there is no silver bullet to solve the structural problem of a widening wealth gap and economic imbalance. There is no individual with a plan or a piece of legislation that will make everything better. The imbalance created by central command does not get solved by central command—quite the opposite. The only real hope is to fix the foundation so everyone can get back to doing the desirable things without the need for conscious control. From there, balance will follow.

But those who clamor for “conscious direction”—and who cannot believe that anything which has evolved without design (and even without our understanding it) should solve problems which we should not be able to solve consciously—should remember this: The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore, how to dispense with the need of conscious control, and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do.

—Friedrich A. Hayek¹⁰¹

With a fixed supply of 21 million, enforced on a decentralized basis and controlled by no one, bitcoin has removed the ability to manipulate the monetary function entirely. What do you do when misbehaving children cannot find a way to share a toy? You take the toy away. The relationship between bitcoin and central banks is similar. Because no human (or institution) can be trusted with control over the money supply, the only practical solution is to remove the ability and temptation altogether. The one constant in bitcoin is its fixed supply. There will only ever be 21 million bitcoin, and there is nothing anyone can do about it. Everything will change around bitcoin, but its supply will increasingly provide the constant from which to measure all other activity. It’s a source of truth that ensures a level playing field. Because the supply of bitcoin cannot be manipulated, neither can its price signal. Undistorted price signals communicate more reliable information. But never confuse more reliable information and a level playing field with price stability or the issue of volatility. If the value of bitcoin is \$12,000 today and \$10,000 tomorrow, that is the undistorted communication of information.

101. Friedrich A. Hayek, “The Use of Knowledge in Society,” *American Economic Review* 35, no. 4 (September 1945): 527.

“Variation is information. When there is no variation, there is no information. [...] There is no freedom without noise—and no stability without volatility.”

—Nassim Taleb and Mark Blyth¹⁰²

A fixed supply ensures that any price change is driven exclusively by a change in demand rather than an artificial and unpredictable change in the supply of money (i.e., communicating a change in preferences to the entire economy). It permanently eliminates an entire side of the equation, which today heavily influences price changes and distorts the communication of preferences. Imagine knowing with absolute certainty that every price change was a product of a shift in consumer preferences rather than the effects of increases or decreases in the money supply. It’s the difference between having true economic price signals to rely on and constantly navigating the unpredictable downstream effects of erratic monetary policy. Today and into the future, the same principle will hold. Everyone will be able to rely on bitcoin’s fixed supply and trust that changes throughout bitcoin’s price system will always be true, free from unpredictable changes in the money supply.

This fundamental difference between the existing monetary structure and bitcoin changes the entire game—false price signals vs. true price signals. False price signals are equivalent to studying for a test believing you have a cheat sheet with the answers, training yourself based on that information, and then showing up only to find out that the test was entirely different. Everyone believes their actions are responses to reliable information (price signals), not realizing the information is being constantly manipulated by changes in the money supply. Each time a violent shock occurs within the system, everyone gets a hint that price signals are communicating bad information. The Fed steps in to stabilize prices, reassuring everyone to carry

102. Nassim N. Taleb and Mark Blyth, “The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous,” *Foreign Affairs* 90, no. 3 (May/June 2011).

on while relying on the same bad information. This process has occurred every time the economy has attempted to rebalance structurally over the past fifty years. It is the primary reason violent shocks to the system are even possible. False signals try to correct, only to be sustained and exacerbated by exogenous forces.

Factors Determining Price & Relative Price under a Constant Money Supply

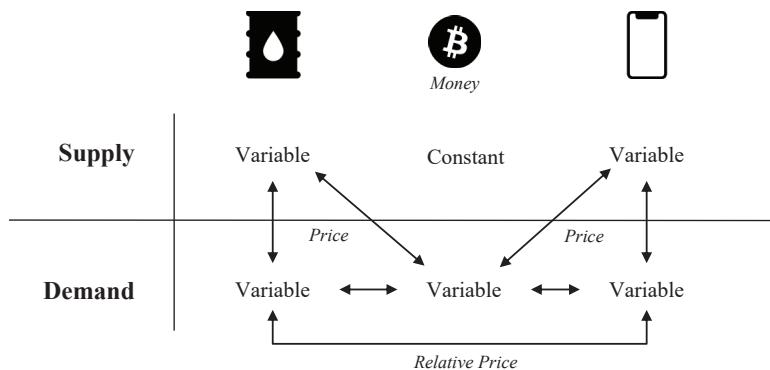


FIGURE 16.13

With a fixed money supply, this wrong is righted permanently. It will no longer be possible to sustain imbalance. So long as bitcoin exists, the monetary medium will not be capable of distributing distorted price signals. There is a difference between right, wrong, and true. True price signals ensure that the information being communicated reflects the individual and aggregate preferences of an economy. In that sense, there is no right or wrong so long as the information can reasonably be relied upon as accurate and undistorted. No one has to trust or question whether bitcoin's price signals are true because its fixed supply guarantees it.

Figuring out how to play a rigged game is no longer necessary because the rigged game is ending. The days of monetary inequity will soon be over as bitcoin distributes throughout the world. It will shift the balance of power back to those that actually create value, as defined by true price signals,

which are communicated by individuals that hold the currency. Setting aside taxes and regulatory capture for a moment, if one wants to acquire bitcoin, he or she will have to provide value in return, and bitcoin will become the arbiter of that value. Of 21 million, approximately 18.5 million bitcoin are already in circulation as of the time of writing. The 18.5 million in circulation are all held by some individual or entity. In order to acquire any, bitcoin must be earned by delivering value to those that hold the currency. Even for those not yet circulating, every single bitcoin must be earned by contributing value. The same is not true of the current monetary system. In the current structure, dollars can either be earned by delivering value to others within the economy, or conversely, if the Fed decides to hand out more money. And this happens quite frequently. Of all the dollars that exist today, over 80% have been created and allocated by the Fed since 2008 (see Figure 16.16), rather than by the alternative—delivering value to others within the economy. Which system sounds more fair, balanced, and conducive to aligning incentives throughout an economy over decades and generations?

As more people adopt bitcoin, the currency is transferred from the haves to have-nots. By making the nominal amount of bitcoin zero-sum, it ensures that the economic system as a whole is non-zero-sum. To join the economy, you must deliver value to someone within the network. No value leaks outside the system. No inefficiency can be introduced through the production of money. Whether new entrants are joining the network or trade occurs between existing participants, bitcoin is always being transferred, and through that transfer, value is actually created. Recall that the valuable function of money is to coordinate economic activity. The production of money, on the other hand, creates no value and only serves to distort and impair the ability of a monetary medium to properly function. The nominal amount of money is not important. What is important is its ability to communicate reliable information and trade value between a broad set of economic participants.

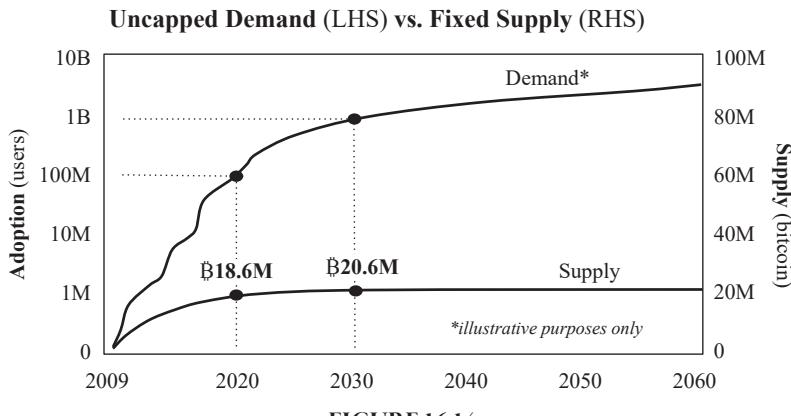


FIGURE 16.14

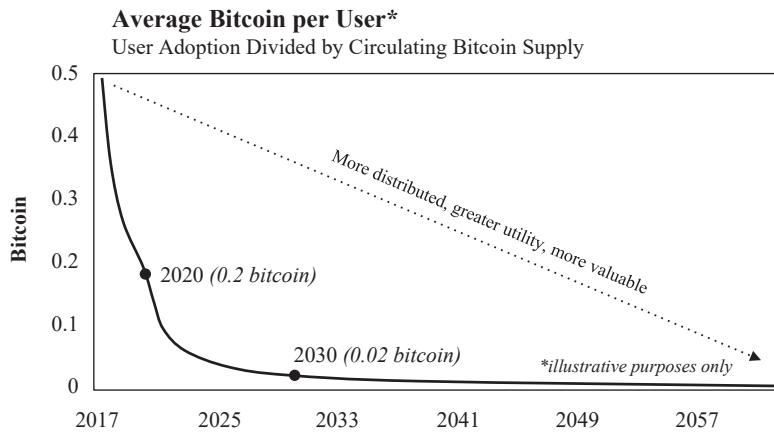
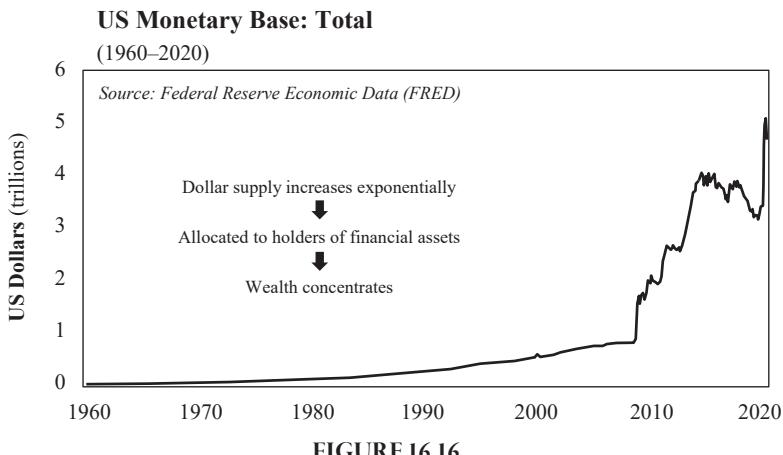


FIGURE 16.15

Money allows individuals to understand the relative value of their output and the relative preferences of others. Bitcoin, with a zero terminal rate of change, enables individuals to make better decisions (on average) in the pursuit of their own interests with more reliable information, free from distortions created by changes in the money supply. A fixed amount of currency combined with a growing number of people valuing it results in increased distribution of the currency over time. No more than 21 million bitcoin will ever exist, and no more than 21 million can ever be saved. Paradoxically, this will drive more people to save as the threat of debasement is eliminated. And as

more people save in a currency with a fixed supply, it results in more and more people owning less and less. But through this function of more people possessing savings, economic stability is created. A fixed money supply naturally causes the currency to become further decentralized and more distributed, delivering greater balance.



Centralized governance of the money supply allows the distribution of new currency units to consolidate, whereas a decentralized governance model enforcing a fixed supply ensures greater distribution of the currency over time. Follow the money. A centralized money supply causes wealth to centralize, and a decentralized money supply causes wealth to distribute. The structure of the currency dictates the respective wealth effects, and this trend can be observed in actual data. Bitcoin held in smaller denominations continues to grow steadily, while bitcoin held in larger denominations continues to decline. As the economic system grows, the currency becomes more widely distributed. The nominal amount held by each individual decreases (on average) while purchasing power increases. As more people demand the currency, its value rises. However, there is a terminally fixed supply. As increased demand naturally outpaces ever-diminishing increases in supply, there becomes one principal way to acquire bitcoin: by delivering

value to an existing currency holder. Over time, the currency transfers from relatively few early holders to a more widely distributed base. Everyone wins. The network utility increases as more participants voluntarily opt in, and the distribution of the currency becomes less and less concentrated, ensuring greater balance and reducing systemic risks posed by the existence of a few extremely large holders.

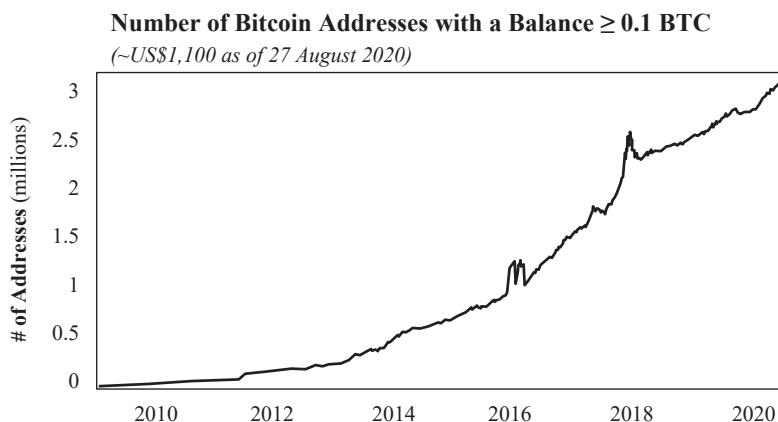


FIGURE 16.17
Source: glassnode.com

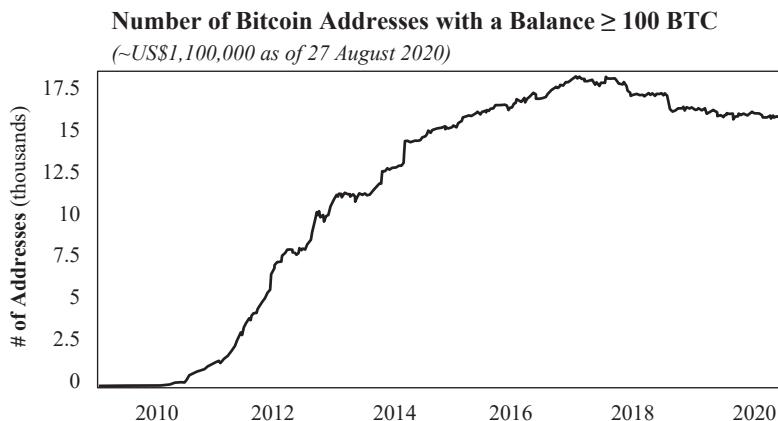


FIGURE 16.18
Source: glassnode.com

When a monetary medium's incentives align individual and aggregate interests, non-zero-sum outcomes become the default, as does balance. Bitcoin is accessible to anyone, and everyone is afforded the same protections. Anyone that produces value and exchanges it for bitcoin is assured that their output will not be devalued in the future merely as a function of someone creating new units of money. Separately, everyone benefits from undistorted price signals. In bitcoin, both rich and poor alike receive these same protections equally. While it is no guarantee that someone else will value the currency more or less, it eliminates the possibility of a forced devaluation of labor and output stored in a monetary medium. In the current economic structure, the wealthiest better understand the effects of active monetary debasement and are best equipped to combat it. Logically, those on the lower end of the economic spectrum have more to gain by leveling the playing field. But fundamentally, it is not about rich and poor. Everyone benefits from the elimination of money production and an economy that provides greater balance, with more reliable information.

Vitalik Buterin @VitalikButerin

Replies to @bitcoinclegane

The idea that an individual can have the immutable right to own a fixed percentage of all the world's money indefinitely, on the other hand, feels very oligarchic.

17 Aug 2018



FIGURE 16.19

In a 2018 tweet, the founder of Ethereum (Vitalik Buterin) beautifully and ironically described the value of holding a currency with a fixed supply that could not be manipulated while arguing for the opposite. He made the precise argument that central bankers use to defend their actions while also articulating the power it would give the individual. While Buterin believes it to be oligarchic to have the immutable right to own a fixed percentage of all

the world's money indefinitely, what if that right were extended to the poorest people on earth? What if it were applied equally to every single person on earth? That is the power of bitcoin. Suppose you live in one of the poorest countries in the Western Hemisphere, such as Nicaragua, and choose to exchange your value for bitcoin. In that case, you now have an immutable right to own a fixed percentage of all the world's money indefinitely. Only you can decide when, how, and to whom to transact for value received in the future. The poorest in Nicaragua are suddenly elevated to the same leveled playing field as a billionaire in New York, such as Paul Tudor Jones. Within the bitcoin network, there is no distinction. Equal rights are the default. This feature cannot and does not exist in the legacy financial system. It is far more oligarchic to indiscriminately devalue someone's monetary savings by increasing the money supply and then choosing who should be rewarded with this new money. There is no comparison between such a world and one where individuals can earn money honestly by producing value for others and are free to determine how best to allocate it for value in the future.

The idea that bitcoin could solve problems today for rich and poor alike stumps quite a few. Most consider bitcoin a speculative asset unfit for people without a certain level of discretionary savings, due to its volatility. It is easy to look at an economic disaster like Venezuela, where the vast majority of people are struggling to have their basic needs fulfilled (i.e., reliable access to food, water, power, and healthcare) and believe there are more urgent concerns than "buying" bitcoin. However, it is hard to ignore the fact that a deterioration in the money caused the economic collapse. Reliable access to food, water, power, and healthcare doesn't exist without the use of money to coordinate resources. The only viable long-term solution is to use a form of money that better fulfills that coordination function. Rebuilding an economy on top of a new form of money requires that someone goes first. Just because it is hard to imagine doesn't change the reality that it's the only way out. One action triggers another and another and another. Whether it's Venezuela, another country suffering from rapid economic deterioration, or any poverty-stricken area in the developed world, the need for assistance is

immediate. But there is no quick fix. Bitcoin can't remove a socialist dictator, it can't take the kleptocrats out of the kleptocracy, it can't reverse damaging tax policy or social programs, and it can't magically turn poor people into rich people or vice versa. However, it can solve problems today for anyone determined enough to use it, regardless of economic status.

The inception point of elevating any individual or society is finding a way to produce more value than is consumed. The best way to accomplish that goal is by using money to exchange value, save value, and coordinate economic activity. Bitcoin isn't just a tool for the rich that will become serviceable to the poor once enough of the rich people have acquired some. That would be nonsensical. There is no reason why a superior form of money would perform one function for some and not others (regardless of wealth, income level, or any other reason). Instead, bitcoin—as that superior form of money—is the best way anyone can level the playing field, irrespective of whether the path may be more challenging for some than others. The demand for money is near-universal, and over time, anyone using the form of money with the strongest foundation and the truest price signals will benefit. The dollar (and all other fiat currencies) benefits a few in the short term at the expense of everyone in the long term. Bitcoin, on the other hand, fixes the economic foundation for everyone. It is one for all.

“Whether in Rome, Constantinople, Florence, or Venice, history shows that a sound monetary standard is a necessary prerequisite for human flourishing, without which society stands on the precipice of barbarism and destruction.”

—Saifedean Ammous¹⁰³

103. Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Wiley, 2018), 30.

PART IV

Conclusion & Acknowledgments

CONCLUSION

Gradually, Then Suddenly

(Authored March 2023)

The Greatest Asymmetry

Asymmetry simply describes anything that lacks symmetry. From a financial perspective, the term is typically used to describe outcomes of disproportionate risk skews. Great upside relative to downside or great downside relative to upside. For example, an asymmetric opportunity might have an upside of 10x or 100x, but you could also lose 100%—10x or 100x up vs. 1x or 100% down. On the other hand, asymmetry can also describe scenarios where there is limited upside and 100% downside. A venture investment in a startup company is positively asymmetric. A startup might fail, resulting in complete loss, but those that are successful typically return orders of magnitude in return. Hyperinflation of a currency is negatively symmetric, with limited upside to holding a depreciating currency and great downside should a currency collapse. Importantly, asymmetry does not in itself have anything to do with the probabilities of individual outcomes, but probabilities remain relevant to risk-taking calculus.

Bitcoin represents the greatest asymmetry that has ever or could ever exist for three principal reasons. The entire world would benefit from a sound form of money that reliably stores value into the future. If bitcoin can *credibly* enforce its fixed supply, it will be demanded by virtually every individual and business in the world. Eight billion people competing for

a finitely scarce resource is massively asymmetric for the early adopters of the currency. Nothing could be more asymmetric than global adoption of bitcoin as money. Second, most asymmetric opportunities are naturally low probability, whereas global bitcoin adoption is increasingly probable. Bitcoin has a known and finite surface area to evaluate. It is binary. Either it can or cannot enforce its fixed supply. As more people adopt bitcoin and as the network becomes more decentralized, the outcome becomes more probable. Third and last, there is inherent negative asymmetry to a currency such as the dollar hyperinflating, which is the other side of the same coin.

The dollar's failure will not be caused by bitcoin, but the two are inextricably linked. To be clear, the problems of printing money are wholly independent from bitcoin. The consequence of printing massive amounts of money out of thin air is hyperinflation. Humans cannot trade their finitely scarce time for something created without any cost or proof-of-work. At the same time, bitcoin was created as a solution to the problem of printing money. Choosing to save in bitcoin is a path to opt out of endless currency debasement. Whatever value is saved in bitcoin cannot simultaneously be saved in dollars or similar depreciating currencies. It is ultimately a choice between one or the other, even if an individual is not 100% exposed to either. Bitcoin is not about making money. Bitcoin is money. And when it comes to any perceived possibility or probability of its ultimate success, the only winning move is to play—an observation Michael Goldstein helped me understand. Given the positive and negative asymmetry on each side, it is not really whether anyone is right but instead, whether you can afford to be wrong.

That is the risk calculus at least, but bitcoin is being adopted as money for very objective reasons. Yes, not everyone that buys bitcoin is adopting it as money. There are people buying bitcoin for irrational reasons or for speculative purposes, without an appreciation for its fundamental bases as money. Both can be true. However, over time, knowledge distributes and fundamentals win out. Cold, hard economic facts dictate human action. Humans need good money to survive. Really, to help fulfill the basic necessities of life

through trade. The world is converging on bitcoin because it is finitely scarce and capable of facilitating direct commerce by and between the largest number of people relative to any other currency system given its permissionless nature. Each individual is a domino. As more dominoes fall, the emergent consensus already forming will become more obvious to more people. In hindsight, the shift to a bitcoin standard will have been obvious. Through the process of mass adoption, bitcoin will transition from a nascent and volatile store of value to a stable form of money used ubiquitously as a medium of exchange and unit of account.

On a Bitcoin Standard

It is fair to say that most people in the world who are conscious of bitcoin think of it as any other speculative financial asset, similar to a stock trading on a computer or TV screen. That is how it appears on CNBC. And the dollar is the *current* unit of account. It is naturally difficult, if not impossible, not to think of bitcoin in dollar terms as a result. However, as global adoption occurs, this too will change. Rather than thinking about the price of bitcoin in dollar terms, bitcoin will become the pricing mechanism. Everything will be priced in bitcoin. That is what it means to become a unit of account. There will be no observable price on a TV or computer screen. Bitcoin will not be principally traded for dollars. Instead, gas at the gas station will be priced and paid for in bitcoin. The same for electricity, water, food and healthcare. There will not be any bitcoin exchanges. Bitcoin will simply help facilitate direct commerce.

On a bitcoin standard, central banks will not be able to print money. Should any country wish to have a central bank as a lender of last resort, it will actually need to be capitalized with real money—bitcoin. Also, the government will not be able to run massive and endless deficits without obvious and more immediate consequences. Governments will need bitcoin to fund their operations, but to do so, any government would have to tax its citizens to get bitcoin rather than rely on a central bank to print money. Nothing

about bitcoin prevents taxes or the establishment of rainy-day funds. Bitcoin also does not eliminate banks. Everything will just have to be done out in the open, funded with actual money. The government will have to directly seek the transfer of bitcoin from citizens via taxes, which are perennially unpopular, and banks will not be able to be bailed out by politicians with money that does not exist. With a fixed money supply, it will be clear that everything must be paid for by someone.

Ultimately, the government will have to compete with the private sector for a finite amount of capital. When money cannot be printed, every economic calculation and decision will be made with greater scrutiny. At a government level, at a company level, and at a personal level. The right to own a fixed percentage of all the world's money indefinitely is not oligarchic. When applied to every last human, it is the most equitable and empowering system ever conceived. The incentive to save will create savers. More people will have savings and fewer people will be in debt. The incentives of the money will dictate it. The output will be an economic system with far greater balance and stability. The banking sector will shrink, and the credit system will be a small fraction of its current size. Lending and capital allocation will still exist, but the banking sector will no longer sit at the epicenter. Without a monopoly on money, banks will have to compete for capital based on value actually added, and all other sectors of the economy will be able to facilitate trade directly without needing to route through the banking system.

Humans will flourish on a bitcoin standard, but there is nothing utopian about it. Running businesses will still be hard, risk will still exist, and the future will remain uncertain. The transition to a bitcoin standard will also not be all roses. It is impossible to seamlessly transition away from a world of excess where the system as a whole is heavily indebted and where very few people have savings. Through a combination of endless money printing by central banks and the world's natural and resulting shift to bitcoin, legacy currencies will eventually hyperinflate. The addict is being taken off the drugs. Society is addicted to debt and money printing as a palliative

means to defer the pain. Sound money is the ultimate antidote, but a period of withdrawal is unavoidable. Things will likely get worse before they get better. Bitcoin will likely even be blamed for the instability created by the volatility of the dollar system. Of course, none of it will be true. The only way out is through a transition to bitcoin. If not for bitcoin, the same inevitable pain would have to be felt from the sins of the past, but there would be no currency to transition to as a reliable or viable alternative.

No matter how uncertain the future or how precarious a transition away from the dollar may seem, bitcoin is the light at the end of the tunnel. It will afford practically everyone in the world with a reliable form of money with which to store and transact value. As Frederich Hayek explained in *The Road to Serfdom*, “money is one of the greatest instruments of freedom ever invented by man.” When governments destroyed money, free citizens of the world took action to reinvent it in a superior form that not even the government could screw up. In doing so, bitcoin will preserve and help rebuild the vestiges of freedom that remain. Money provides an economic tool and incentive to create value for those around you. It allows for a range of choice and wealth unimaginable just a few hundred years ago. Freedom is the ability to pursue whatever interests you may have in this world, and money provides a medium to be compensated for those interests, in a way that can be carried indefinitely into the future. At its most fundamental core, bitcoin is money, and it is the greatest instrument of freedom ever invented by man.

Acknowledgments

I could never have written this book without the many people who collectively helped educate me or who otherwise influenced my thinking about bitcoin originally. Will Cole, Saifedean Ammous, Napoleon Cole, Marty Bent, Michael Goldstein, Marcus Dent, Pierre Rochard, Jimmy Song, Brooks Dudley, Vijay Boyapati, Stephan Livera, Andreas Antonopoulos, and Wences Casares are among many of those who contributed directly or indirectly to my understanding as I went down the bitcoin rabbit hole.

I began writing the original series of essays when I worked for Unchained and owe a debt of gratitude to the entire team for having supported me. As co-founders of Unchained, Joe Kelly and Dhruv Bansal trusted me to represent the company and gave me full discretion to share my unedited views of bitcoin. To differing extents, many of my conclusions and perspectives were and inevitably still might be controversial—to the world generally, within our industry, and even within our company (at least at the time). *Gradually, Then Suddenly* might never have seen the light of day with different founders and within a different company.

When I originally wrote the bulk of my work, Phil Geiger, Will Cole, and Adam Tzagournis were my primary sounding boards for editorial feedback. Their comments sharpened my thought processes and improved my writing. In the process of writing the book version, Anil Patel and Neil Woodfine were instrumental in the editorial process and significantly improved the polish of the final work to make it worthy of print. It would have never have become

a book had each not shouldered a heavy load when they did. In addition to the substantive editing process, Anil helped create all the graphics. Anil has a special skill of distilling complex thoughts into both visualizations and written copy. In many ways, I view this book as a collective work of both of ours because the images and graphics help tell a story that is otherwise much more difficult to grasp. Through the process of completing the book, Jimmy Song served as both an accountability partner—as he wrote his latest book, *Fiat Ruins Everything*, which you should also read—and as a mentor, which was invaluable to me in creating steady forward progress.

Over the past nine months, I have written and otherwise worked on this book out of the Bitcoin Commons in Austin, Texas. While there is no singular bitcoin community, there are local bitcoin communities all over the world, and community is important to bitcoin. I view the Bitcoin Commons as a model for bitcoin communities everywhere to replicate. The space would not exist without the Austin bitcoin community, and it would not be possible without the support of a broad set of bitcoin companies, including Unchained, NY-DIG, Ten 31, Swan, Spiral, Strike, Priority Power, TFTC, Trammel Venture Partners, Fold, Satoshi Pacioli, *Bitcoin Magazine*, Braiins, Casa, and Trezor. I specifically want to thank Kaily Buemi, who helps run the Bitcoin Commons, as well as Justin Moon, the Godfather of Austin Bitdevs. Without Austin Bitdevs, there never would have been a Commons. And without the Commons, I wouldn't have had a space to write with the bitcoin community around me as a support structure and source of inspiration.

This is my first and hopefully last book—I will be a one-hit wonder if I'm lucky. In the middle of my self-publishing process, I had to audible and hire a team of independent freelancers. Saifedean Ammous was incredibly generous in providing me with advice and recommending resources that he used in publishing *Principles of Economics*. I am grateful for the editing support from Tara Taylor and Renata Sielecki, work on citations by Holly Gorman, and the design skills of Lorie DeWorken. The collective efforts of these individuals allowed me to improve the overall body of my work and are credited with ultimately helping me turn my writing into a professional

and polished work product that I was proud to publish and put in print. The original cover art was created by Proof of Paint, specifically as a commission for *Gradually, Then Suddenly*. I want to thank the artist who worked tirelessly to create a beautifully unique piece and fittingly, who wishes to remain pseudonymous. The art is an allegory of the individual's journey to bitcoin, which we collaboratively created to fit hand-and-glove with the book. It turned out to be the perfect finishing touch to bring everything together.

I also want to thank Grant Gilliam, Scott Shreeve, Alex Gladstein, Peter McCormack, Ross Stevens, Bruce Gutkin, and Brett Morrison for reviewing and providing valuable feedback. While there are too many bitcoiners to thank them all, I do want to mention a combination of friends and friends in spirit who have either influenced me or had a lasting impact on my bitcoin journey—directly or indirectly—and who I haven't already mentioned: Buck Perley, Ben Carman, Gideon Powell, Cam Stromme, Trey Sellers, Justine Harper, Michael Tanguma, Annaliese Wiederspahn, Tyler Campbell, Velvet Campbell, Daniel Chavez, Griffin Haby, Dave Hogan, Mario Gutierrez, Sahil Chaturvedi, Paul Miller, Tony Giorgio, Nick Gates, Gigi, NVK, Giacomo Zucco, Rockstar Dev, Aleks Svetski, John Magill, Alan Lane, Matt Odell, Erik Cason, Brady Swenson, Sam Callahan, Preston Pysh, Rod Bitkite, Gary Leland, Alex Leishman, Jack Mallers, Christian Keroles, Yan Pritzker, CJ Wilson, Ted Rogers, Cory Klippsten, Natalie Brunnell, Jeff Vandrew, Michael Saylor, Max Keiser, Stacy Herbert, Mark Moss, Bryan Bishop, Ti Kawamoto, Mitch Klee, Ryan Gentry, Michael Atwood, Michael Flaxman, Away Slice, Tuur Demeester, Nate Kitzke, Andrew Poelstra, Brandon Quite, Guy Swann, Daniel Prince, and Steve Barbour.

To all the bitcoiners who have shared with me that the original essays helped you on your journey to understanding bitcoin, thank you! It is the best compliment I can receive when it comes to my work, and it was inspiration for the book. Lastly, I want to thank my family and closest friends. Bitcoin might be the most important tool ever invented by man, but it is just a tool. It would mean nothing without the people in my life who make it all worthwhile.

FIGURES

- 0.1. Central Bank Balance Sheets 2009 vs. 2019
- 0.2. Emerging Market Currencies vs. USD 2009–2019
- 1.1. Decision Tree: Bitcoin’s Path to Global Reserve Currency
- 1.2. Factors Determining Price & Relative Price under a Constant Money Supply
- 1.3. Value Creation and Communication through a Single Monetary Medium
- 1.4. Creating Order through Measurement
- 1.5. Network Adoption and Possible Network Connections
- 1.6. Dollar, Euro, Yen, and Gold Indexed to Bitcoin, 2014–2019
- 1.7. Uncapped Demand vs. Fixed Supply
- 1.8. Average Bitcoin per User
- 1.9. Global Bitcoin Reachable Nodes Map, November 2019
- 1.10. Annual Rate of Currency Supply Change: Bitcoin, USD, Yen, and Euros, 2011–2019
- 1.11. Bitcoin Volatility: Present vs. Expected Future
- 1.12. Network Value Size and Implications for Participants
- 2.1. Selection of Books on Bitcoin
- 2.2. Independent Verification of Blocks by Nodes
- 2.3. Valid Block Construction (selected elements)
- 2.4. Proof-of-Work Function (simplified)
- 2.5. Bitcoin Supply Curve with Halving Epochs
- 2.6. Acceptance and Rejection of Proposed Blocks at Halving
- 2.7. Blockchain Decision Tree (sourced from *The Bitcoin Standard* by Saifedean Ammous, 2018)
- 2.8. Bitcoin Adoption Flywheel
- 2.9. Technology/Globalization Plane (adapted from *Zero to One* by Peter Thiel, 2014, p. 8)
- 3.1. Purchasing Power of Bitcoin in US Dollar Terms, May 2019–September 2019

- 3.2. US Debt (systemwide) (Fed Z.1 report) and Nominal GDP (FRED website), 1987–2018
- 3.3. US Debt (systemwide), Nominal GDP, and Federal Tax Receipts indexed to 1987 levels
- 3.4. Debt Securities and Loans and Monetary Base, 1986–2018
- 3.5. US Monetary Base (annotated with quantitative easing rounds), 1959–2019
- 3.6. Contrasting Monetary Systems: Centralized vs. Decentralized
- 3.7. Bitcoin Supply Curve with Halving Epochs
- 3.8. Bitcoin Hashrate, 30-Day Moving Average, 2018–2019
- 3.9. Acceptance and Rejection of Proposed Blocks at Halving
- 3.10. Mining Decision Tree: Valid vs. Invalid Work
- 3.11. Address Derivation for Private Key: Public Keys, Address, Signature
- 3.12. Economic Incentives of Bitcoin: Checks and Balances
- 4.1. Monetary Systems: Centralized vs. Decentralized
- 4.2. Bitcoin vs. Fiat across Cost, Benefit, and Volatility
- 4.3. Tweet by Ted Rogers, 6 September 2017 and 23 April 2018
- 4.4. Bloomberg News Coverage of India’s Cryptocurrency Ban, 3 July 2018 and 4 March 2020
- 4.5. Bitcoin Market Dominance, 22 August 2019
- 4.6. Tweet by Pirate Beachbum, 25 May 2020
- 4.7. Bitcoin/USD Price, January 2020–April 2020
- 4.8. Tweet by Hal Finney, 10 January 2009
- 4.9. Tweet by Nicolas Dorier, 17 August 2017
- 5.1. Consumer Price Index: Purchasing Power of the Consumer Dollar, 1980–2020
- 5.2. The Dollar Hamster Wheel
- 5.3. Tweets by Nic Carter and Pierre Rochard, 30 November 2020
- 5.4. Sources of Global Debt, 1999–2017
- 5.5. Net Assets of Mutual Funds in US (2002–2019)
- 5.6. Net Assets of ETFs in US (2002–2019)
- 5.7. US Finance & Insurance Sector as Share of GDP (1970–2020)

- 5.8. Tweet by Dave Portnoy, 4 June 2020
- 5.9 Distribution of US Wealth, 1989–2020
- 5.10. US Savings Accounts by Size, November 2019
- 5.11. Uncapped Demand vs. Fixed Supply
- 5.12. Market Value of Negative-Yielding Bonds, Bloomberg Barclays Global-Aggregate Index
- 5.13. Global Government 10Y Bond Yields, 20 December 2020
- 5.14. Cycle of the Great Definancialization
- 5.15. Tweet by Michael Saylor, 9 November 2020
- 6.1. US Monetary Base (Total) January 1959–July 2019
- 6.2. Attempts to Copy Bitcoin
- 6.3. Emergent Properties of Bitcoin
- 6.4. Bitcoin’s Value Function Reinforces Credibility of Supply Schedule
- 6.5. Blockchain Decision Tree (sourced from *The Bitcoin Standard* by Saifedean Ammous, 2018)
- 6.6. The Minority Rule by Nassim N. Taleb
- 7.1. Consumer Price Index: Purchasing Power of the Consumer Dollar, 1980–2020
- 7.2. Tweets by European Central Bank, 12 March 2019 and 9 July 2019
- 7.3. BTC/USD Price Chart Log Scale, 2011–2019
- 7.4. Bitcoin’s Value Function Reinforces Credibility of Supply Schedule
- 7.5. Fixed Supply vs. Expanding Demand
- 7.6. Stages of Technology Adoption (S-Curve)
- 7.7. Bitcoin Adoption Waves (Simplified)
- 7.8. Changes in Bitcoin Demand, Supply, and Value, 2016–2019
- 7.9. Aggregate Wealth Stored in Bitcoin vs. Assets of US Households
- 7.10. Bitcoin Volatility: Present vs. Expected Future
- 7.11. ALT 60/40 Portfolio Return Profile vs. 1%, 3% Bitcoin Allocations, VanEck, 2019
- 7.12. Bitcoin’s Path to Full Monetization
- 8.1. Bitcoin Hashrate, 30-Day Simple Moving Average

- 8.2. Venezuela Monthly Crude Oil Production, 2000–2019
- 8.3. US Monetary Base (Total) with QE, January 1959–July 2019
- 9.1. Jacob Leupold, “Steam Engine,” *Theatri Machinarum Hydraulicarum II*, 1720.
- 9.2. Innovation vs. Scaling
- 9.3. Technology/Globalization Plane (adapted from *Zero to One* by Peter Thiel, 2014, p. 8)
- 9.4. Bitcoin White Paper, p. 1 (cropped)
- 9.5. Selected Block Data for Blocks 591,272–591,274
- 9.6. Bitcoin Blockchain Size, August 2017–August 2019
- 9.7. Bitcoin Halving Schedule, Eras 1–5
- 9.8. Legacy Payments Flow Chart
- 9.9. Payments Layer as a Bridge for Money
- 10.1. Pick your Narrative
- 10.2. Is Bitcoin for Criminals? Decision Tree
- 10.3. Silk Road Payment System, 2015
- 10.4. Tweet by Hal Finney, 10 January 2009
- 10.5. Decentralization Spectrum
- 11.1. Banning Bitcoin Decision Tree
- 11.2. Bitcoin FUD! Dice (v2) by Nic Carter, 2019
- 11.3. Bitcoin vs. Competing Monetary Mediums
- 11.4. Global Bitcoin Reachable Nodes Map, November 2019
- 11.5. Monetary Systems: Centralized vs. Decentralized
- 11.6. Banning Bitcoin: Prisoner’s Dilemma
- 11.7. Tweet by Michael Goldstein, 14 January 2019
- 12.1. Comparing Bitcoin and the US Dollar: Supply, Issuance, and Governance
- 12.2. US Dollar Historical Supply and Bitcoin Supply Schedule
- 12.3. Total Bitcoin in Existence, September 2019–October 2019
- 12.4. Verification of Bitcoin Supply and Issuance Rate on a Bitcoin Node, Block Height: 599,114

- 12.5. Purchasing Power of Bitcoin Relative to Dollars: BTC/USD, November 2011–May 2020
- 13.1. Tweet by Lawrence H. Summers, 22 August 2019
- 13.2. The Central Bank Playbook
- 13.3. Comparing Purchasing Power of the US Dollar with Monetary Base
- 13.4. Comparing Debt Securities and Loans with the Monetary Base
- 14.1. Other Factors Supplying Reserve Balances: Total Factors Supplying Reserve Funds
- 14.2. Cash Assets, All Commercial Banks (US), 2014–2020
- 14.3. S&P 500 Index, December 2019–April 2020
- 14.4. Bitcoin Supply Schedule by Year (projected)
- 14.5. Bitcoin/USD Price Chart: January 2020–April 2020
- 14.6. The Gonzales Flag, painted by Cynthia Burns and Evaline DeWitt, 1835
- 15.1. Fed, ECB & BoJ Combined Balance Sheet: Total Assets, January 2008–April 2020
- 15.2. Tweet by Michael Goldstein (@bitstein), 15 September 2018
- 15.3. US Labor Force vs. Fed Balance Sheet, 2008–2020
- 15.4. New US Dollars Added into the Financial System, 26 February 2020–29 April 2020
- 15.5. US Credit System Leverage Dynamics After New Dollars Added
- 15.6. Consumer Price Index: Purchasing Power of Consumer Dollar in US City Average
- 15.7. Total US Debt System-Wide vs. Fed Balance Sheet Assets, 2005–2019
- 15.8. US Credit System Expansion and Federal Government Share of US Credit System
- 15.9. US Total Monetary Base and Bitcoin Supply Schedule (updated)
- 15.10. Purchasing Power of Bitcoin Relative to Dollars: BTC/USD, November 2011–May 2020
- 16.1. Distribution of US Wealth, 1989–2020
- 16.2. US Savings Accounts by Size, November 2019
- 16.3. US Weekly Jobless Claims vs. S&P Index, January 2020–July 2020

- 16.4. Portrait of Bitcoin Sign Guy during Janet Yellen's 2017 HFSC Testimony, by Jim Ferguson
- 16.5. Value Creation and Communication through a Single Monetary Medium
- 16.6. Mortgage-Backed Securities Held by the Federal Reserve: All Maturities, 2007–2018
- 16.7. US National Home Price Index, Home Ownership, Labor Participation, 2007–2019
- 16.8. Relative Size of an Economy vs. People Distorting the Economy
- 16.9. US Credit System Leverage Dynamics After New Dollars Added
- 16.10. Debt Securities and Loans; Liability, Level, All Sectors, 1945–2020
- 16.11. Labor Productivity vs. Hourly Compensation, 1948–2014
- 16.12. US House Price Index vs. Housing Opportunity Index, 2000–2019
- 16.13. Factors Determining Price & Relative Price under a Constant Money Supply
- 16.14. Uncapped Demand vs. Fixed Supply
- 16.15. Average Bitcoin per User
- 16.16. US Monetary Base, Total, 1960–2020
- 16.17. Number of Bitcoin Addresses with a Balance ≥ 0.1 BTC, 27 August 2020
- 16.18. Number of Bitcoin Addresses with a Balance ≥ 100 BTC, 27 August 2020
- 16.19. Tweet by Vitalik Buterin, 17 August 2018