BUILDING CONFIDENCE IN

BLOCKCHAIN



INVESTING IN CRYPTOCURRENCY
AND A DECENTRALIZED FUTURE

CARTER L. WOETZEL

BUILDING CONFIDENCE IN BLOCKCHAIN:

INVESTING IN CRYPTOCURRENCY AND A DECENTRALIZED FUTURE

CARTER LEE WOETZEL



NEW DEGREE PRESS
COPYRIGHT © 2020 CARTER LEE WOETZEL
All rights reserved.

BUILDING CONFIDENCE IN BLOCKCHAIN:
Investing in Cryptocurrency and a Decentralized Future

ISBN

978-1-64137-920-5 *Paperback*

978-1-64137-691-4 *Kindle Ebook*

978-1-64137-693-8 *Ebook*

"It is mutual trust, even more than mutual interest, that holds human associations together."

—H. L. Mencken

To my siblings, cousins, friends, teachers, parents, aunts, uncles, and grandparents. You have made me who I am today. A special thank you my sister Meckenna, your sometimes hidden love for writing inspired me to begin this journey long ago. Garrett Woetzel, for sending me down a life-changing rabbit hole.

Grandpa Osborn, your patience and wisdom has given me a healthy dose of caution. Professor Holland, for converting me into someone passionate about finance. And finally, to Mr. Fedor—for believing in a kid from a small town called Ham Lake.

INTRODUCTION

BLOCKCHAIN AND TRUST

You let out an impatient sigh as you hit the "Parking Ramp" elevator button. You had a long day of meetings at work, and your spouse just texted you that they need you to pick up a gallon of milk. You unlock your car, turn the ignition, and are off to the races. Weaving through traffic and what feels like an innumerable amount of traffic lights, you drive over a bridge that takes you to your local grocery store. You park the car, lock it, and walk through an automatic sliding door. Quickly selecting a gallon of milk, you hand your credit card over to the cashier and are soon on your way. You are ten minutes late for dinner, but you trust your spouse does in fact still love you despite your many apparent flaws.

In a simple mundane journey of a perfectly normal day, you take many leaps of faith. You trust that the elevator won't crash, that you will arrive on the corresponding floor of the button you hit, that the car door will unlock, and that the vehicle will start. You trust others not to run a red light and smash into you when the light turns green (a rather unnerving contract with society). You trust the bridge you crossed to be properly maintained so it doesn't collapse. You locked your car in the grocery store parking lot because you don't quite trust that every single person has your property's best interest in mind. You trust those automatic sliding doors to activate upon your arrival. You trusted the milk on the shelf to not be spoiled, and the cashier to not steal your credit card information. Finally, you trusted that your spouse would still love you despite arriving late to dinner!

Trust is all pervasive: inescapable in our daily transactions and movements. Trust is the most valuable resource of the twenty-first century. It is the digital oil that all infrastructure, interactions, and communication are built on top of. Every Amazon purchase, credit card swipe, and meal consumed hinges upon trusting either a source or an action will result in a desired outcome. We surround ourselves with routines, ideas, and people we trust. It is an integral part of the human experience for better or for worse.

As you read this book, you will develop an understanding of what I call the "Trust Problem." It is intertwined with many businesses and third parties that exist to facilitate and ease the worries of our daily transactions. News alert—the current way of dealing with the Trust Problem is less than ideal! Trust is an issue that is pervasive in every transaction between humans. Blockchain is the answer to the Trust Problem, turning the tables on society's antiquated method of transacting. Instead of trusting people, **what if we can trust the guarantee of mathematics and the neutrality of automation through programming for our transactions and contracts?**

Before we begin this journey together, I want you to understand what brought me to the table. Three years ago, my cousin Garrett Woetzel (a finance savant) linked me to a variety of articles on this thing called "blockchain." As an undergrad getting a degree in finance and computer science, the appeal of this packaged deal of digital currency, decentralized ledger technology, cryptography, economics, and all the investment hype drew me in. I was like an eager bee ready to taste the mysterious nectar known as "blockchain."

As I joined a variety of projects in the space and began to invest, a lot of commotion occurred. Prices skyrocketed nearly 700 percent for a variety of cryptocurrencies—and subsequently plummeted.

Communities I had engaged with had people who turned into millionaires, and shortly thereafter were utterly broke. Parents who enthusiastically jumped in because their kids recommended it walked away defeated. As I consumed all the literature I could get my hands on in the cryptocurrency and blockchain space, I found that none of the books struck a balance between the pessimism of investing fundamentals with the enthusiasm for what could be unlocked in the near future with blockchain and cryptocurrency.

That is what set me on this journey. This is what drove me to read hundreds of research papers written by some of the most brilliant researchers in the world. Over the course of three years, I built for myself a rock-solid understanding of blockchain and cryptocurrency with the goal of making this emerging technology understandable for everyone. That is what this work is: a comprehensive dive into this emerging technology in a simple fashion by **equipping you to understand, explain, and invest in blockchain technology.**

THE COMING EXPLORATION

Arthur C. Clarke once wrote, "Any sufficiently advanced technology is indistinguishable from magic."[1] Blockchain technology is no different relative to the mystery surrounding it. Leveraged as a marketing term or headline buzzword, blockchain and cryptocurrency have soured for a huge percentage of the population.

Maybe you have heard of cryptocurrency (such as Bitcoin), or maybe you haven't. Perhaps you invested and got burned during the 2018 bubble. Or maybe you are a traditional investor that wants to learn what all the fuss is about. Regardless, you will walk away from this book understanding that in the near future, blockchain will be whirring away in the background of our lives—just like the internet. And, what's more, you have a chance to invest in the infancy of this

emerging technology that solves the Trust Problem that is so prevalent in our world today.

This book will give you clarity in a space that repeatedly misses the mark on educating readers to a point of confidence. By the time you are done reading this book, you will be able to confidently answer the following:

- Why is blockchain valuable?
- How does blockchain work?
- How should I invest in cryptocurrency and a decentralized future?
- What is the past and future of blockchain technology?

But what exactly *is* blockchain? And why should you care?

"Blockchain is shorthand for a suite of distributed ledger technologies that can be programmed to record and track anything of value, from financial transaction to medical records or even land titles."[2]

—LUCAS MOSTAZO

The first chapter, **Blockchain & *Ventre à Terre,*** is devoted to answering the question, "What is blockchain and how does it work?" For now, you just need enough to know that blockchain is a digital decentralized ledger that is maintained by thousands of different computers. Picture a decentralized version of PayPal, but with a lot more capabilities and many valuable properties that centralized services cannot offer.

This ledger leverages cryptography and mathematics to guarantee the validity of transactions and to remove power from any single third party (such as a bank or Facebook). Users who use the blockchain ledger can transact in a peer-to-peer fashion with 100 percent confidence the digital transaction or contract will complete successfully, without any human interference.

THE TRUST PROBLEM AND SKEPTICISM FACTORS

The foundations of blockchain were first splattered in digital ink onto a screen in 1979 by David L. Chaum in his PhD dissertation paper, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." This humble title says a couple of critical things. First, the original value of blockchain is centered around trust between groups of individuals who have no way of trusting each other. In other words, **blockchain exists to solve the problem of trust between mutually distrustful parties.**[3] The apps and businesses that are using blockchain are using the technology to solve the problem of trust. The conquering of the Trust Problem makes blockchain valuable.

Every use case (the way the technology is used) is built upon the following simple set of questions. What is not trusted? How does blockchain create trust in the situation that would not be possible without a blockchain?

The original ideators built blockchain off of the understanding that humanity lacked a technology that could facilitate transactions while simultaneously being trustless, decentralized, and censorship resistant. These ideas are revolutionary, and the ideators that created the possibility of such a technology did it on the back of mathematics, game theory, and software, fully knowing their work would change society. As David Chaum noted in his introduction for the original piece of research literature that would lead to blockchain, "Manuel Blum was around a lot that summer, and he and I talked. He maintained that one should never try to predict the effects of one's actions on society. It was the rejection of this principle which led to the present work."[4] Little did Chaum know just how much that paper would change the world.

Talking to various investors, professors, and technology enthusiasts (many of whom are hesitant about cryptocurrency and blockchain) has led me to many intriguing conversations. Spectator investors who have long been entrenched in traditional investments are consistently reluctant about cryptocurrency. I have been able to narrow these down to what I like to call the "Skepticism Factors," of which there are three: **Volatility, Trust, and Tangibility.**

Investments that are built on products in flux—without a firm place in society—are volatile. Cars are a stable part of society; we will always need to get from point A to point B in some capacity. A car's valuation typically doesn't change from $100,000 to $5,000 in a couple of days. The value of any given car is, for the most part, relatively mapped out. Housing and shelter will always play a part in human existence, and probably McDonald's too. Let's be honest, cheap and quick food isn't disappearing anytime soon. These examples are all mapped out, "stable" investments. The revenue streams are fairly easy for investors to track.

Blockchain technology, which enables cryptocurrency, is not so. We are in the stage of unknown unknowns when it comes to adoption and integration. The cryptocurrency market also lacks liquidity. This makes cryptocurrency as an investment speculative, risky, and volatile. **But just because an emerging technology and asset class justifiably contains volatility within price discovery does not detract from the legitimacy of the innovation in progress.** It merely adjusts the expected return of the investment.

The irony of the second problem—trust—is blockchain exists to solve this exact problem. For as long as humanity has been around, third parties have existed to facilitate transactions and the execution of contracts. Real estate escrows, debt collection agencies, attorneys, landscaping companies, and marketing agencies—all of

these require trust. Often, this trust is quietly misplaced and exploited.

What if there were an alternative to trusting people? A perfectly neutral party that could always be trusted? This is what blockchain enables—mathematics running monetary policies, programs executing transactions, and contracts being enforced digitally. All operate without needing to trust a human party—trustless trust.[5]

Thus, I was left to grapple with "tangibility" as the indescribable problem many high-caliber investors—potentially including you, the reader—have with cryptocurrency. When I asked a retired finance professor why he was so pessimistic about the future of cryptocurrency as an asset class and product, he immediately looked uneasy. Perhaps his voice even contained a trace of disgust: "You can't touch it. There seems to be a lot of hand-waving. This whole cryptocurrency thing . . and blockchain is just not tangible."

Lack of tangibility came up interview after interview until it could be ignored no longer. Some of these people were modern individuals, children of the digital era. How could they be so obtuse about wanting the product to be tangible?

In the middle of the summer of 2018, I set out for a ten-mile run with my mind set to this question. Running often produces a meditative state in which everything seems to quiet down. It's my favorite pastime and problem-solving tool, and a painful one at that. As I passed by a small pond, I spotted a swan standing perfectly still. I kept running. I'm not one to slow down for anything. An oncoming car drove by me and grabbed my attention for a couple of seconds. I glanced back at the pond.

The swan was gone.

The moment felt magical. I knew that swan was real. It had to have been. I trusted my eyes. I trusted what I saw. Trust. Trust is what made that mysterious swan feel tangible.

In many ways, I would argue **trust itself is an attribute of tangibility.** If we see something in front of our eyes, we move through space trusting that the information we receive is true. Anyone who has used virtual reality before can relate to the confusion of this fact suddenly not being true. The verification of reality no longer matching the information from your own eyes is chaotic and disorienting. Thus, **trust seems to be the step between tangibility and verification.**

If you've ever made an online order before, when you put your card number in and commit a transaction, you trust the product will eventually end up on your doorstep. I would imagine that the first time individuals made online orders, they did not trust the product would arrive. Thus, the original people who made online orders took a risk and were eventually rewarded by a product conveniently arriving on their doorstep (verification). The more a user purchases online, the more we take the transaction itself as something tangible. If you make an Amazon order and you click on the "Add to Cart" and "Purchase," a twenty-first century user would say the entire exchange feels "tangible." Perhaps this is because there is a series of mouse clicks. Regardless, **the outcome builds trust, which eventually converts into a feeling of tangibility.**

Digital banking is not tangible. You cannot touch a transaction because "transacting" is a verb. Yet we take leaps of faith every day when we swipe our cards here and there. The result of the swipe is tangible, and the transaction is therefore tangible. **The twenty-first century economy of transactions will be invisible and pervasive. If you do not deny digital banking as being tangible,**

then don't be contradictory and claim decentralized ledger technology (blockchain) and cryptocurrency are "not tangible." You simply trust one and not the other.

Thus, to anyone who felt cryptocurrency is not tangible, such as our retired finance professor mentioned earlier, I posed the following question: "Have you transacted on any blockchain before using cryptocurrency?"

The inevitable answer was "no." As someone who has transacted over six hundred times on a variety of blockchains, one of my goals for this book is to get you to experiment and use cryptocurrency. It is one of the quickest ways to understand the breadth, magic, and possibility this emerging technology is capable of achieving.

CENTRALIZATION VERSUS DECENTRALIZATION

What are the systems you trust today in the world? At this very moment, how much does the world know about you? Do you trust the companies and apps you use? How much say do you get in your control over your own assets and data? If today the bank decided your account had zero dollars in it, what would you do? If Facebook decided to sell all your profile information and location data to the government, or if your phone company traded your everyday conversations to a third party, what could you possibly do to stop this? What control do you truly have?

You are not at the top of those hierarchies. You are merely a participant.

As I began to investigate the original research papers on Bitcoin, blockchain, and privacy, it became clear to me that centralization of power is a lurking beast we as a society have decided to trust. And rightfully so—centralization was created out of a time when no

effective alternative problem-solving solution existed. Since then, centralization has shape-shifted to meet the many demands of society.

"Centralization itself is not evil—it cannot be. It does not exist in opposition to anything. It's just a concept, a point on a line, always in relation to something else. Over-centralization is the enemy—cycles of reconcentrating power amongst fewer individuals until systems collapse under their own weight."[6]

—TOR BAIR OF ENIGMA MPC (BLOCKCHAIN)

Centralized systems on the surface are not inefficient, from an economic standpoint. The problem with centralization is not efficiency, but the characteristics that are born out of an overcentralized system.[7] Because of the relationship between centralized systems and the user, oftentimes the user has no effective alternative that does not contain the negative externalizations. For the longest of time, the negative externalizations of overcentralization posed a trinary choice: participate, choose a lesser evil, or sit out completely. Centralized systems are often imposed on individuals as a result of historical events they are wholly unaware of. Terms and conditions apply.

The US monetary system is centralized.[8] Internet service providers are centralized.[9] Your entertainment is centralized (Disney and Fox combined own 35 percent of the movie market).[10] The servers holding your information for Snapchat, Facebook, and Instagram are centralized.[11] Even farming in the twenty-first century is centralized![12]

Centralized systems are a natural human reaction to any sort of chaos that involves a large number of parties needing to come to consensus on how to do an action efficiently, and, in many cases, to

"serve the customer." No wonder the majority of businesses are authoritarian in structure.[13]

Yet just because something is natural does not mean it is fair. And just because something is efficient for some does not mean it is efficient for all. Decentralized systems such as blockchain are an alternative solution to centralization, a solution created by human tendencies designed to solve the problems of the first millennium.[14], [15] Enter the twenty-first century, when we face problems inconceivable to past generations. The stakes are higher and a trusted alternative to centralization is desperately needed.

"A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."[16]

—SATOSHI NAKAMOTO, ANONYMOUS CREATOR OF BITCOIN

This book grapples with this topic. At our fingertips is a technology that solves the problem of distrust, centralization, and the possibility of executing transactions and contracts digitally without a centralized intermediary. Blockchain opens the door to truly peer-to-peer transactions, without human intermediaries sucking up value along the value chain of simply transacting from one person to another. Blockchain is not without its flaws; one of the economic levers that gives blockchain the ability to solve these problems (cryptocurrency) is in a constant state of fluctuation. But on a

horizon not far from here is a world where those levers are stable, and the technology underneath emerges as a beautiful solution.

The time for top-down abstraction of what blockchain solves is over. Let us now begin the journey of answering the burning question on your mind. "Enough of the suspense. What the heck is blockchain? And how does it work?"

---

1 Lucas Mostazo, "What is BLOCKCHAIN? The best explanation of blockchain technology," YouTube video, 6:26, January 14, 2018, https://www.youtube.com/watch?v=3xGLc-zz9cA.

2 Arthur C. Clarke, *Profiles of the Future: an Enquiry into the Limits of the Possible (*London: Pan, 1983).

3 David Chaum, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups," (PhD dissertation, University of California, Berkeley. 1979).

4 lbid.

5 Ed Featherston, "Blockchain: You Want Me to Trust a 'Trustless Trust' System?" Last Modified November 15th, 2017.

6 Tor Bair, "The True Enemy of Decentralization," Last Modified February 26, 2018.

7 lbid.

8 Olya Green, "RE-imagining Money: Are the 700 Years of Centralization over Now?" *Hacker Noon*, May 6, 2020.

9 Vince Tabora, "The Evolution of the Internet, from Decentralized to Centralized," *Hacker Noon*, October 27, 2019.

10 David Sims, "Hollywood Makes Way for the Disney-Fox Behemoth," *The Atlantic*, Atlantic Media Company, Last Modified March 21, 2019.

11 "Why Decentralizing Social Media Makes Sense," *Social Media Explorer*, November 20, 2018.

12 Kendall Thu, "The Centralization of Food Systems and Political Power," *Culture & Agriculture* 31, no. 1, June 8, 2009.

13 Clay Fuller, "The Economic Foundations of Authoritarian Rule," (PhD dissertation, University of South Carolina, 2017).

14 Sueur Cédric, et al. "From Social Network (Centralized vs. Decentralized) to Collective Decision-Making (Unshared vs. Shared Consensus)." *PLOS ONE*, vol. 7, no. 2, 2012.

15 AlgoShare, “To Centralize Is Human, to Decentralize Divine,” Last Modified November 20, 2018.

16 Satoshi Nakamoto, “Bitcoin Open Source Implementation of p2p Currency,” Satoshi Nakamoto Institute, Last Modified February 15, 2009.

CHAPTER 1

BLOCKCHAIN & *VENTRE À TERRE*

"Sorry to be a wet blanket. Writing a description for this thing for general audiences is bloody hard."[17]

—Satoshi Nakamoto, anonymous creator of Bitcoin

When I first set out to describe blockchain in a simple fashion, I spent months poring over the original research papers: David Chaum's 1977 dissertation, Satoshi Nakamoto's 2008 white paper, Vitalik Buterin's Ethereum whitepaper, and a list that could go on for quite a while.[18], [19], [20] I wasn't satisfied. I extended my search to simplified explanations: an example of this was the University of California Berkeley's 2015 "Blockchain Technology—Beyond Bitcoin" paper.[21] Even YouTube videos such as "Blockchain Explained Simply" contained a surprising amount of chaos in comment sections. [22] People didn't seem to understand. Even if they did, they didn't have the confidence to echo it back at others.

The realization during my research was this: we are not taught the concept nor logistics of ledgers, and because blockchain is just a radically futuristic ledger, the dilemma the majority of people encountered on their first attempt to learn about blockchain became rapidly apparent.

We know how to go to the gas station and purchase a soda, but we don't really stop and think how this transaction is recorded by the gas station, the bank, and all of the intermediaries that take a slice of any given transaction. At best, the average person tracks how the balance in their account/ledger increases or decreases. We are stuck viewing the world using a single-ledger paradigm.

Understanding ledgers is the first step in comprehending blockchain. **A ledger is a living record of financial transactions.** You use ledgers every single day and other ledgers are at play other than your own account that are an integral part in confirming your own account

balance in what I like to call the "ledger ecosystem." Because truthfully, your current balance of $34,220 in your bank account is merely the sum of all the transactions that have been coming to and from your account.

The paycheck from your company adds +$832 to your account (of which the company's ledger reflects -$832), the transfer to your PayPal account nets -$150 on your bank account (with PayPal's ledger gaining +$4.99 for the transaction fee), and the outbound transaction to buy that Big Mac is -$2.32 (+$2.32 on McDonald's ledger). **Your own account balance you use every day is a simple ledger interacting with hundreds of other ledgers that are constantly reconciling and balancing with each other.**

This is the starting point of understanding blockchain. We need to start viewing the world as hundreds of different ledgers constantly reconciling and balancing with each other, with many centralized ledgers of dollars being the centralized point of authorization and ownership. Additionally, not all ledgers are created equal. Some have more power than others. And this is true of not just banks, but any sort of mass data system. Databases (Facebook servers, Twitter, eBay, or Amazon) are merely ledgers of data instead of ledgers of dollars. All of these are centralized intermediaries that attempt to facilitate transactions between two parties.

With the current system, many ledgers are centralized in their control over many people's dollars and data, introducing the risk of manipulation and distrust. This is why we have accountants and audits all the time (which are quite expensive). We come to find out that reconciling disputes between huge centralized ledgers is expensive. **Centralized players do not like trusting each other. The whole system is built on a shaky system of trust.**

“ . . . the duplicate and time-consuming post-trade processes that banks, brokerages, custodians and clearing houses undertake to reconcile multiple ledgers represent a very large cost of trust embedded in the existing system”[23]

—CENTER OF ECONOMIC POLICY RESEARCH

A DECENTRALIZED SOLUTION

But what if there were a way for truly peer-to-peer interactions between you and me or between businesses without any sort of human third party intermediary slowing down and sucking up value along the way? What if you and I truly controlled our own accounts? What if there were a system, backed by mathematics and cryptography, that everyone could trust as the facilitator of transactions in an entirely automated fashion that we know to be secured, auditable, and permanent?

That is precisely what blockchain does. Blockchain flips the centralized ledger paradigm on its head.

We now know what blockchain exists to solve, but what precisely is blockchain?

Blockchain is a decentralized ledger of transactions, accounts, and data secured by a decentralized ownership of the ledger, in which mathematics and cryptography are the digital law of the ledger. The maintenance and use of the shared ledger is made possible within the ecosystem using digital cryptocurrency as the medium of exchange, which is simultaneously the incentive for those who maintain and secure the ledger to continue to do so.

Instead of trusting a chain of centralized parties to backup, update, and verify your own transactions and your own wealth, we instead trust publicly visible coded protocols to manage and maintain our transactions. The digital laws of the ledger are built with mathematics—a perfectly neutral party we can all trust as the facilitator of truly peer-to-peer transactions.

What's more is that the control of the digital ledger and its rules are made up of a decentralized community—stopping any single party from manipulating the rules of the ledger or the ledger entries. Because everyone has the same copy of the ledger, it becomes easy for protocols to spot anyone who attempts to manipulate the ledger.

In the end, leveraging public-key cryptography (the same stuff that makes the internet work) allows everyone who uses this decentralized ledger to now make peer-to-peer transactions without the need to be reliant on multiple intermediaries to make a simple transaction possible.

HOW DOES BLOCKCHAIN WORK?

You're with a group of friends and you decide to loan ten dollars to your friend Austin. Your two friends Dakota and Tony see this transaction take place and take note of it mentally. A week later, Austin pays you eight dollars and says, "That's how much I owe you." Naturally, you are upset! What is the proof that Austin has returned the wrong amount? Dakota and Tony back you up: "It was ten dollars —we were there when you made that transaction." As a friend group, the accepted consensus is that Austin owed you ten dollars, not eight. Your group has created a **pseudodecentralized ledger** in which each party is cross-checking to make sure the record of transactions is kept fair and balanced.

Also known as a Decentralized Ledger Technology (DLT), blockchain is a system of record keeping in the form of a digital ledger.[24]A blockchain has the following set of properties: the ledger is distributed, shared, immutable, and composed of cryptographically linked entries in the ledger that take the form of "blocks." The protocol—the coded law that controls how the transactions and balances are maintained and executed on the ledger—is designed to continuously build consensus on what the shared ledger contains at any given moment.[25]

Your friend group of twenty people decides to make its own currency. We will conveniently call this currency "cryptocurrency." You've decided the only way anyone is allowed to transact with each other is if everyone is present for the transaction, and the majority of the people will allow the transaction to be made. **Everyone records the same transaction on their own personal ledger. Using this system, everyone has an identical ledger, and consensus is maintained.** If Tony purchases an item for ten dollars from Dakota, all twenty people will record this transaction in their own ledger.

If anyone attempts to change their balance on their ledger from ninety to one hundred dollars, the next time they attempt to trade or transact with someone else in the group, all other parties individually own their own identical "shared" ledgers that point to the fact that the individual does not have a ledger that matches the rest of the group. Because the group catches a mismatch in ledgers, the person is then punished with some sort of fee and is not allowed to trade with anyone else until they adopt the ledger that the rest of the group is using. This is another feature of blockchain: **it eliminates the danger of any single party manipulating the ledger in their favor—creating a more secure network of transactions than a traditional centralized system.**[26]

We have highlighted the following valuable features of a blockchain ledger: **consensus, enhanced security, corruption resistance, distributed ledger (by design), and decentralization of power.** This leaves the following features of decentralized ledgers: immutability, auditability, and permissionless participation to be examined and explained.

THE PERFECT DATA FINGERPRINT

The council of twenty friends decides to sit down and figure out a way to make the process of seeing if everyone's ledgers match easier. You are three years in, and what was once a small notebook for a ledger has now turned into a thick dictionary of transactions. People are concerned a majority of the twenty individuals could collude to make a series of changes in the ledger from the past and have that corrupted ledger become adopted, robbing the innocent and enriching the nefarious actors.

What if there were a mathematical way to ensure no entries in the past could be changed? This guarantee would give the decentralized ledger the property of immutability.[27] What's more, could that mathematical surety become a part of the protocol "law" that automatically and "trustlessly" ensures no one can game the system?

This is where the power of programming and mathematics crosses over. **A "hash" function is the perfect mathematical solution to this exact problem.** Hashing is the algorithmic process of turning a given set of data into a unique digital fingerprint in the form of a perfectly unique string output. This function works no matter how big or small the data input is. Tom Scott, a web developer and owner of the famous YouTube channel "Computerphile," explains it as follows: "A hash algorithm is kind of like the 'check digit' in a barcode

on a credit card . . . The last digit in a barcode on a credit card is determined by all of the others digits."[28]

An example of using Secure Hashing Algorithm 256 (SHA-256) is as follows:

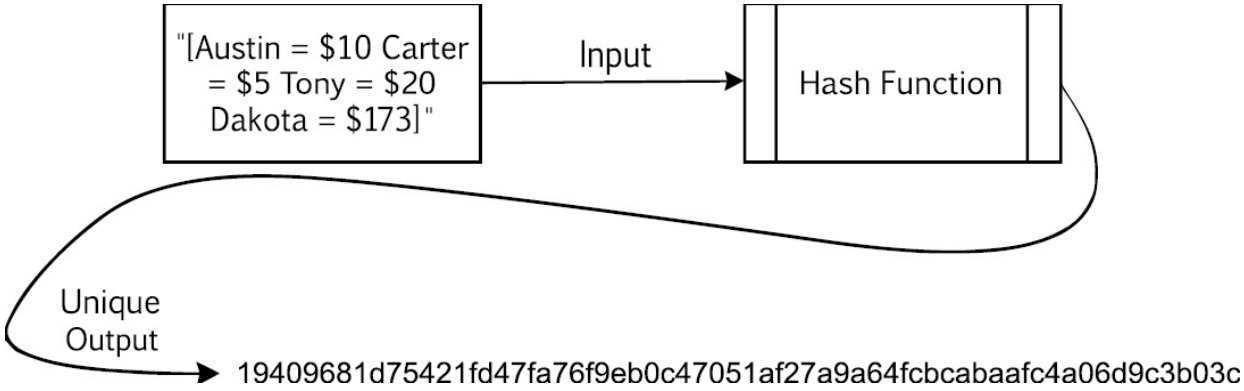


Figure 1: SHA-256 Hashing Example

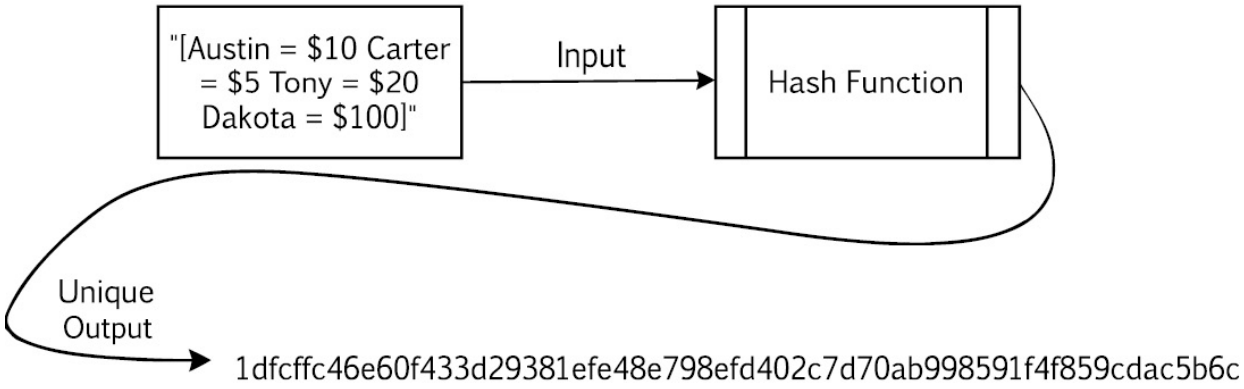


Figure 2:SHA-256 Hashing Example with Changed Input

"[Austin = $10 Carter = $5 Tony = $20 Dakota = $173]" as input.

SHA-256 hash of the input = 19409681d75421fd47fa76f9eb0c47051af27a9a64fcbcabaafc4a06d9c3b03c

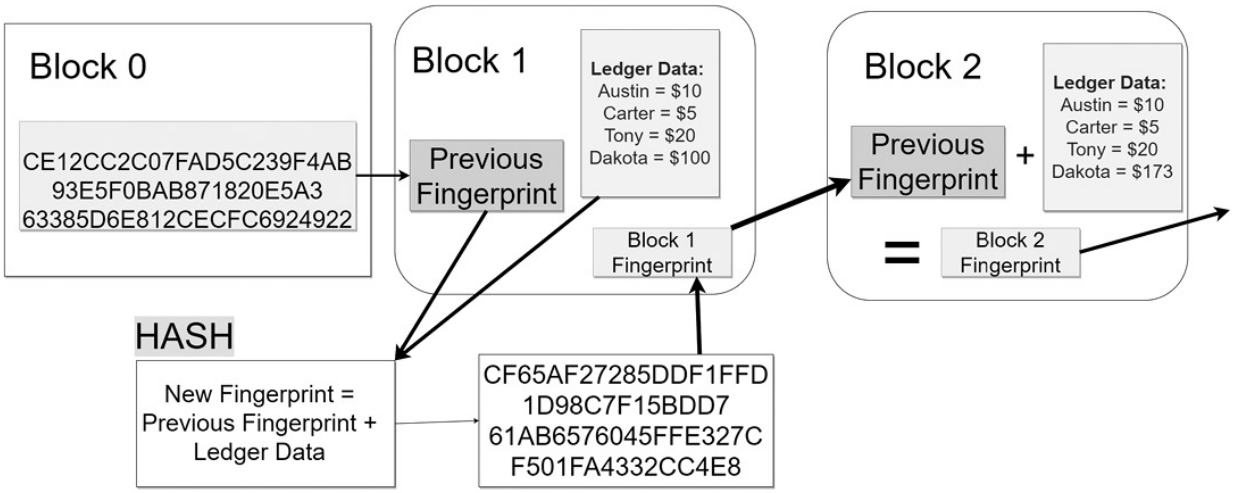
"[Austin = $10 Carter = $5 Tony = $20 Dakota = $100]" as input.

SHA-256 hash of the input = 1dfcffc46e60f433d29381efe48e798efd402c7d70ab998591f4f859cdac5b6c

Any changes to the data, in this case Dakota's total money as $100 instead of $173 (sent in as input to the hash function), produces a drastically different fingerprint. That is remarkable. You could enter a one hundred thousand-page dictionary into a hash function, **and if someone changed even a single word in the dictionary or character anywhere in the dictionary, the output will be visibly different than the original hash of the entire dictionary.** This is jaw dropping. It is utterly shocking—the type of fact that makes me pause and ponder the beauty of mathematics and research that makes this possible. Hashing gives a mathematical guarantee; a way for computer systems and people to know with 100 percent confidence that a given set of data has not been tampered with in any capacity.

Before we incorporate "hashing" into our circle of friends, we need to think about the difficulties. Hashing an entire ledger or dictionary of transactions takes a significant amount of time. What if a quicker way existed? This is where "blocks" enter the playing field. We make a simple rule. No one is allowed to go back into the history of the ledger to change any records. If you break this rule, it will be easy to spot.

Here is how: Everyone starts a new distributed ledger, same as before. Every page of this new ledger contains a set of records and account balance updates. When a new page or "block" is created, **the hash of the previous page of data is stamped onto the new page.** We do this again and again as more transactions and pages are added to everyone's identical ledgers/books. This means every new page contains a perfectly unique fingerprint created by the fingerprint from the previous page of the ledger.



Example 3: Chain of Fingerprints

You cannot recreate these "hashed" fingerprints on each page unless you have an identical history of data and fingerprints from all of the previous pages or "blocks." This is the guarantee generated from these blocks/pages "chained" together using a hash function. Thus, the name "blockchain" is used.

This chain of records, known as blockchain, is a mathematical guarantee that gives an extremely convenient method for checking that the decentralized digital ledger has been unaltered. Instead of comparing every single page and entry, we now have a single value on the most recent page of the ledger all twenty friends can compare with. Simply compare the most recent hashed page of transactions. No human party needs to be trusted with making an error during the check. It's math. One plus one equals two. Forever and always. Trustless trust.[29]

This mathematical guarantee, in combination with the design of decentralized ledgers, creates trust—simultaneously giving the property of both **immutability** and **auditability**.[30] The blockchain is immutable because the past financial records cannot be altered without destroying the chain of fingerprints, and thus the validity of any nefariously changed ledger (in comparison to the agreed-upon

distributed ledger everyone else is using) is destroyed and ignored. Because the past is unalterable, you can easily flip through the pages/blocks of the ledger and observe the entire perfect unaltered history of transactions and balances within the ecosystem. Zero arguments result about who traded with whom and for what amount. All transactions are in the blockchain ledger. Publicly visible. Perfectly auditable. Concrete in immutability.

Finally, what does it mean for blockchain to be **permissionless**? Simply put, **anyone** can join your circle of twenty friends. Anyone can trade with anyone. You are free to transact within the rules of the protocol. In a digital sense, this means anyone with an electronic device, internet connection, and a "wallet" (of which there are many) connected to your favorite blockchain allows you to immediately participate in an entire ecosystem. This setup is as simple as downloading a browser extension or installing an app on a phone that is designed to be integrated into a blockchain.[31] You are permissionless in that you have complete agency separate from any centralized authority. There are no complex forms to be filled. No credit scores. Nothing. You can jump straight into transacting with others in a peer-to-peer fashion.

What does this look like tangibly? Well, I am two clicks away on my computer from opening my secure crypto wallet on a Chrome browser. This crypto wallet is also on my phone. The user interface is no different than Venmo; I can interact with websites, games, and apps that are integrated on a blockchain, all of which are designed to take advantage of the properties of blockchain. I can send cryptocurrency anywhere, to anyone in the world, at any time: peer to peer, whenever I want. I can use decentralized exchanges that are entirely automated and out of the control of a single party. I can take out collateralized loans in a blink—no paperwork. I can partake in derivative markets from scratch in a couple of seconds using Augur. I

can purchase from traditional stores with crypto—over fifteen thousand vendors globally accept cryptocurrency, including Wikipedia, Microsoft, Expedia, AT&T.[32] I can digitally tip an author of an article I like. And the list goes on.

This is all seamless, all integrated on the blockchain, and none of it looks wildly different than our current web browsers. You will still have your phone apps and your websites. What is different is the degree of freedom and functionality you have by simply having a crypto wallet. Anyone with an internet connection can start one—zero paperwork.

What characteristics of blockchain are the catalyst for this greater degree of freedom and functionality? **Consensus, enhanced security, corruption resistance, distributed ledger (by design), decentralization of power, immutability, audibility, and permissionless in nature are the fundamental components that give blockchain technology (and by extension cryptocurrency) intrinsic value.** These are the attributes that separate the systems that can be built with decentralized ledger technology, or blockchain, in contrast to many of the centralized systems that exist today.

Welcome to a decentralized future.

DECENTRALIZED VALUE

Blockchain at its core is a digitally distributed record-keeping system in which any individual in the world who has an internet connection can partake in updating and verifying these shared digital records.

With digital banking, you have an account number with a balance. Anytime you make a transaction, the bank updates the centralized ledger by keeping track of the exits and entries of your digital cash movement and changing your overall balance accordingly.

Traditionally, in order to be able to send money to someone else or transact between parties, a series of links are set up: your bank to PayPal or a debit card, and then that information entered on a centralized platform such as Amazon or eBay. If a customer purchases from another customer, banks down the chain must communicate and complete the transaction on their own ledger after leapfrogging from the platform facilitating the transaction.

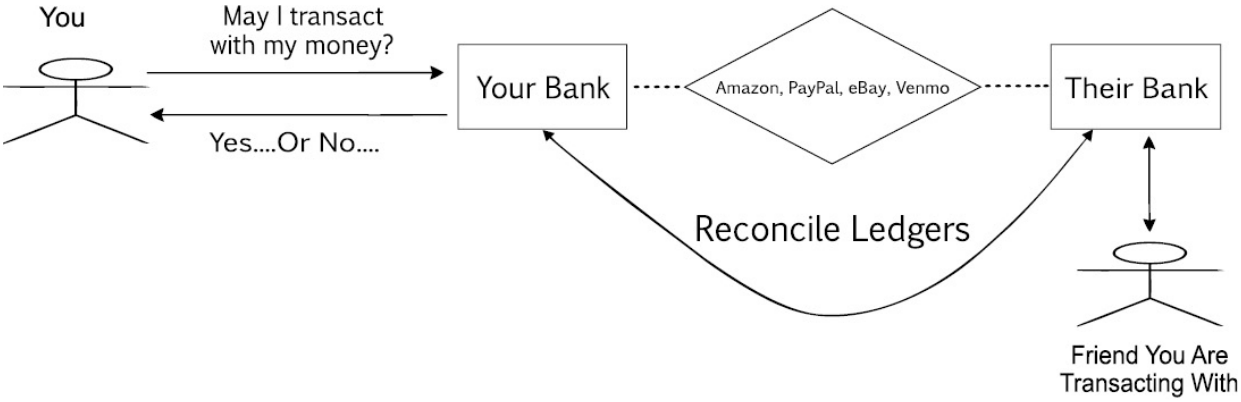


Figure 3: Centralized Ledger

Instead of trusting a chain of centralized parties to backup, update, and verify your own transactions, we instead hand over control of the digital ledger to a decentralized community, making all transactions peer to peer, updating the shared ledger universally instead of funneling through a series of centralized intermediaries.

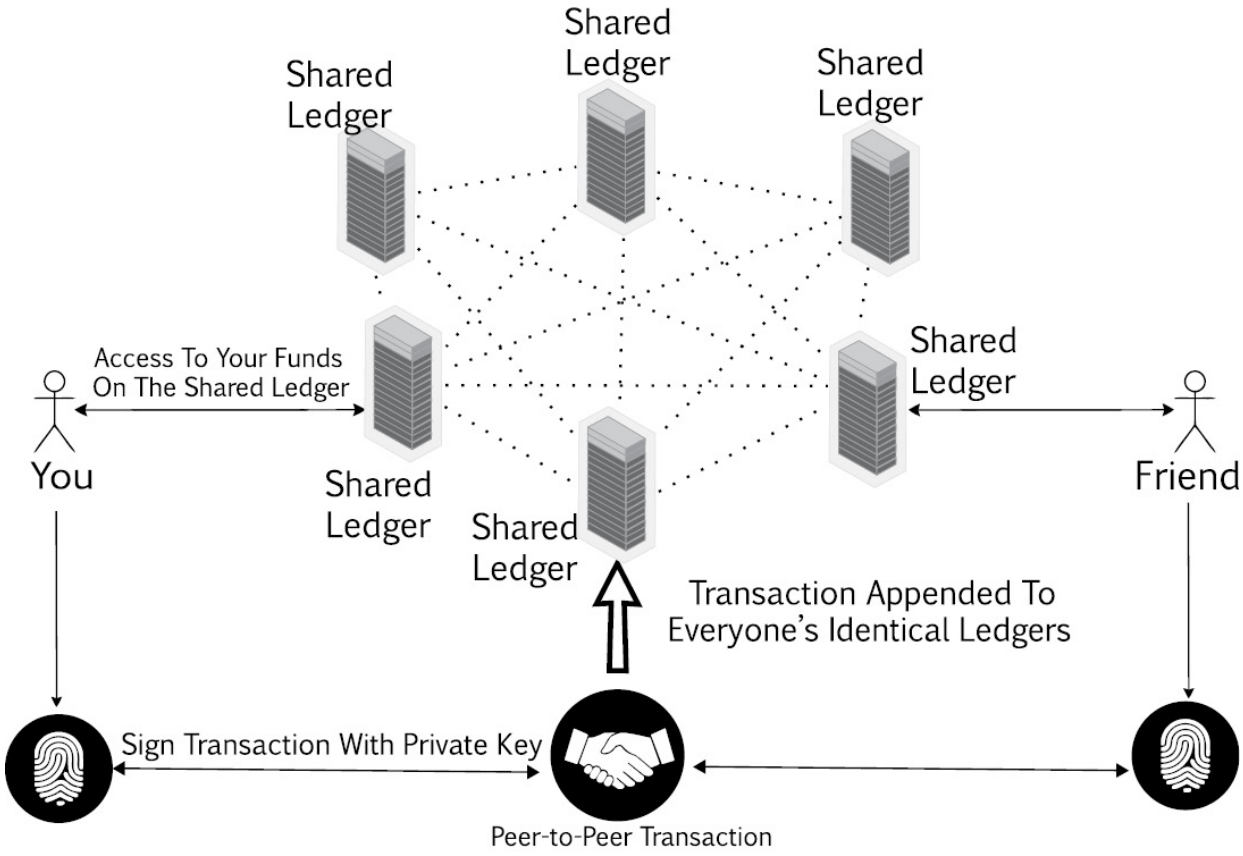


Figure 4: Decentralized Ledger

No longer do you need to hand off the question of "one plus one equals what?" to the bank. You don't even need permission from the bank to ask that question! Instead, you have agency and control over how much cryptocurrency you will send and where you will send it. The decentralized group of nodes that support the distributed ledger answers "one plus one equals two" as a collective unit—drowning out any single nefarious actor who attempts to answer with "three" instead. This contrasts with a centralized ledger, which could answer "three" without any challenge, damaging your personal ledger and trust in the system.

What makes this shared ledger valuable from a business perspective? The distributed ledger is valuable because it is publicly maintained, agreed upon, and decentralized in its ownership. In the twenty-first century, the majority of records are maintained, updated, and sold by

a single party.[33]This is expensive for anyone who needs to use the records held by a centralized party, and leads to trusting a human organization to be ethical and consistent with the data. In addition, centralized players have a hard time trusting other centralized parties' ledgers of data. Lo and behold, even the biggest players don't trust each other!

Let me paint a picture. You open your bank account and attempt to wire $50,000 to your "friend" in South Africa (looking at you, Nigerian prince email scammers). The transaction gets flagged and blocked by your bank. In addition, something went wrong. The money was accidentally subtracted from your account. You then engage in a long legal dispute in which you attempt to prove ownership of the money with receipts and checks to a court. The bank's ledger gets final say, and you are left grappling with the ramifications of never truly having control of your own money.

There are a couple of frustrating pieces at play here. Why can't you send your money anywhere in the world to anyone? Why do you have to prove ownership to someone else who is merely the custodian of your assets? Why do you have to interact with so many third parties in the process of attempting to prove what you own and what you were trying to transact?

What happens if we were using a blockchain for this transaction instead? You would simply open your digital crypto wallet (of which there are many) and send $50,000 worth of Bitcoin to your friend's public wallet address (similar to a mailbox, but on digital highways instead). In the process, you would incur a micro fee to pay the decentralized nodes on the blockchain network that facilitates the transaction. The transaction will either happen or it won't—binary in its execution.

No gray area and no possible transaction limbo exist. Either your assets are transferred, or they are not, all of which is recorded publicly on the blockchain. There is no need to go to a third party. Your ownership of the assets is already recorded on the blockchain, just as your transfer of ownership to your friend in South Africa is recorded onto all of the identical decentralized ledgers distributed globally.

This is all seamless: no single third party and no centralized ledger. Your decision to transact was permissionless. The ability to control what you want to do with your own assets was not contingent on a third party. The power was entirely in your hands—facilitated by a decentralized network.

GEARS AND LEVERS

Now we rewind the clock. How was that transaction possible? If every transaction is added to the chain of records, and everyone must be on the same page for a decentralized digital ledger to work, how in the world do we come to a conclusion as an entire group?

The answer is once again "consensus." There are hundreds of thousands of nodes, or computers, that all have the same copy of the digital ledger. Whenever someone wants to make a change to the ledger, more than 50 percent of this decentralized network must agree to make the change. This is no different than an election, and much of the economic groundwork reuses the principles of normal elections.[34]

This should be slightly alarming to you. Couldn't someone arbitrarily set up an enormous number of nodes and take control over more than 50 percent of the network? If the network has the attribute of being "permissionless," indiscriminately allowing anyone to join in on maintaining the ledger, how would this attack be stopped? If the

majority of the network decides a certain crypto wallet should move an asset from address A to B, then that is precisely what will happen —with or without the wallet owner's consent.

This is called a Sybil attack.[35] It is known as a "51 percent attack." **This was the final problem in the blockchain space to be solved before a blockchain could truly exist.** What is stopping someone from forging multiple identities to influence the consensus process?

This is where the brilliance of the anonymous Satoshi Nakamoto, creator of Bitcoin, bridged this torrential issue in 2008. You see, up until 2008 a huge number of the components to make a blockchain reality were researched and possible to implement. The 51 percent attack was a fundamental bottleneck that remained to be solved. How do we stop a Sybil attack? How do we stop people from gaming the consensus system?

What Satoshi Nakamoto realized was that no cost was attached to gaming the consensus system. Game theory made it easy to break consensus. A finite resource that has real-world value needed to be sacrificed in return for the ability to publish a set of transactions to the chain of records.

Nakamoto solved the problem by engineering a solution known as the proof-of-work consensus model (PoW).[36] In order to propose a transaction or change to the digital ledger, a price must be paid to the network in the form of computation power, or electricity. Computation in PoW is spent on solving a puzzle that takes a significant amount of electricity to solve. This is where the term "mining" was introduced. Anyone can strike gold and solve the puzzle, but those who commit more resources are more likely to hit a vein of gold.

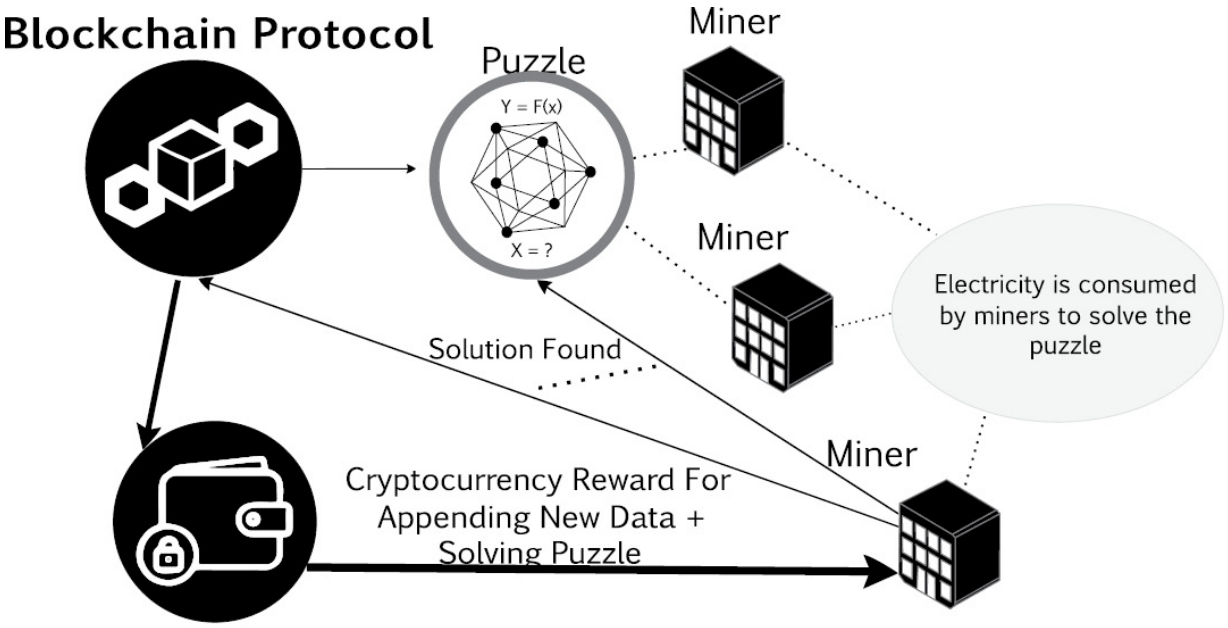


Figure 5: PoW Mining

Ultimately, the goal of this mining incentive-cost system is that no one entity can, over time, take over record updating (block production) because of the vast amount of resource consumption required. What is more, the number of wallets or identities that were created on the blockchain no longer mattered—consensus was now based on a cost. **Proof-of-work does not pay nefarious actors, only those that contribute to the continued success of the ledger.** Using the proof-of-work consensus model, blockchains could finally be permissionless while simultaneously containing strong deterrents against malicious attempts at breaking consensus.

The most brilliant detail Nakamoto devised is that the difficulty of the puzzle is automatically adjusted based on the total amount of computation power attempting to solve the puzzle—the more nodes solving the puzzle, the more difficult the algorithm becomes.[37] **When the puzzle is solved, the block (or page) of transactions the "miner" is attempting to add to the ledger becomes the de facto newest block appended onto everyone's ledger.** A ledger/miner refusing to adopt the newest block would be ignored—the "hashed"

fingerprint on the most recent pages would no longer match all the other identically distributed ledgers.[38]

By only having one block/page of ledger updates be added at a time (roughly every ten minutes for Bitcoin), another problem is solved—time-stamping problems. If more than one block could be added at the same time, the "double spend" problem would result. If a user submitted two outbound transactions from their balance using the same set of Bitcoin on the ledger and sent this to two different blocks at the same time, we'd encounter an issue of ordering. One of those transactions should be allowed through, and one of them not, or else the user gets to "spend the same dollar twice" and break the fairness of the cryptocurrency. **By only having one block of changes made to the ledger at a time, the blockchain design solves the "double spend" problem by having the protocol automatically check for double spending within the single proposed block, while not having to deal with the timestamping conflicts if multiple blocks were allowed to be appended at the same time, which is impossibly difficult.**[39]

But what if this newest single page/block is nefarious? What if all the other "pages" of the ledger are correct, except the most recent block proposed?

This is where public-key cryptography saves the day again.[40] Every crypto wallet/address has a private key—similar to a Social Security number or your fingerprint. Whenever a transaction is made outbound from the address/balance, the transaction must be "stamped" by this private key in order for the transaction to be accepted into the proposed block. Essentially, it's mathematically impossible to get away with "stamping" an outbound transaction with a fake private key. The protocol verifies that the owner of the address signed the outbound transaction with a private key. If not,

the proposed block is immediately ignored and tossed out. The bad actor loses money in the form of wasted expenditure on electricity and may become "white-listed" and ignored by the rest of the network: a permanent punishment dealt by miners who truly support the blockchain.

I should note that, within the consensus system, the modified SHA-256 puzzle algorithm creates a lottery dynamic in which someone who has one "vote" can absolutely solve the puzzle versus someone with ninety-nine "votes'" worth of computation power. This is simply to say the answer to the puzzle is randomly distributed using elliptic curve cryptography, and this randomness cannot be gamed.[41] More computation will increase the frequency of winning, but the distribution of the solution to the puzzle is still random.

The proof-of-work consensus model to date has worked perfectly—534,500,000 transactions exist on Bitcoin's blockchain, with over thirteen thousand new transactions appended per day to the Bitcoin ledger.[42], [43] The more individuals transact on a blockchain, the greater the native cryptocurrency of the respective blockchain is priced. A high price incentivizes more miners to attempt to solve the puzzle and be the miner that submits the new block to the ledger. The reason for this is twofold. Miners that solve a puzzle and publish the newest-appended block to the to-be-adopted ledger earn revenue in the following ways:[44]

1. Rewarded the transaction fees from everyday people like you and me who want to trade, transact, or update the ledger in some capacity
2. Rewarded automatically by the protocol a certain amount of cryptocurrency for each puzzle solved and new block submitted

This creates ferocious competition among miners to be the selected miner. **The more individuals compete to be the winning miner,**

the more decentralized the consensus becomes and the more secure the network is. A beautiful side effect of price increasing for any cryptocurrency is it encourages more miners to attempt to solve the puzzle, ultimately securing the ledger. This is because it becomes more expensive to game the system with more competition while simultaneously increasing the decentralization of the network by having more nodes with their redundant copy of the universal ledger sustaining the decentralized ledger.

TRANSACTION

But what if I don't want to pay these vast electricity costs to attempt to solve the puzzle and have my transaction posted to the blockchain? What if I just want to transfer or transact with my cryptocurrency like how I use PayPal?

This is precisely where "miners" come in handy! First, you submit your transaction to the "pending transaction pool." This pool is where your transaction is verified as legal by the protocol's definition. Along with your submission to this pool, you set a reward for any miner who publishes your transaction. Picture this as a pizza tip in which all the drivers in the area know how much you are going to tip (versus someone else). **Those who submit higher "tips" are going to have their transactions published sooner.**

Multiple miners will pick up your transaction if they deem your tip adequate and add it to the "block" of transactions that the individual miner is attempting to add to the ledger. A Bitcoin "block" can contain five hundred transactions.[45] Different blockchains, such as Bitcoin Cash, have larger block sizes, allowing more transactions to be published to the ledger per block. If the miner solves the puzzle, the new set of records is appended to the currently agreed-upon chain of records, and the miner is automatically paid the "tips" as

well as a protocol reward of cryptocurrency for solving the puzzle to compensate for computation costs. Voilà! Your transaction is now submitted and etched into history, and the miner walks away a happy camper.

You now have a firm grasp of how this complex but beautiful beast known as blockchain works. Other consensus models other than proof-of-work are used by different blockchains. Despite some trade-offs to these (proof-of-stake, proof-of-authority), ultimately all of these consensus models exist to give the blockchain the valuable attributes mentioned earlier.[46]

Consensus, enhanced security, corruption resistance, distributed ledger (by design), decentralization of power, immutability, audibility, and permissionless in nature are what make cryptocurrency and blockchain valuable. As we eventually turn to cryptocurrency as an investment, these valuable principles of decentralized ledger technology will be used in various apps and businesses to solve the problems of the present and future.

---

17 Satoshi Nakamoto, "Re: Slashdot Submission for 1.0," Satoshi Nakamoto Institute, Last Modified July 5, 2010.

18 David Chaum, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups,"(PhD dissertation, University of California—Berkeley, 1979).

19 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshi Nakamoto Institute, Last Modified October 31, 2008.

20 Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," (Whitepaper, 2014).

21 Fthi Arefayne Abadi, Joshua Ellul, and George Azzopardi, "The Blockchain of Things, beyond Bitcoin: A Systematic Review," (Abstract, 2018).

22 Y0coin, "Ted Talks: The Blockchain Explained Simply," December 23, 2016, Video, 15:31.

23 M., Casey, J. Crane, G. Gensler, S. Johnson and N. Narula, "The Impact of Blockchain Technology and Finance: A Catalyst for Change," *Geneva Report on the World Economy No. 21*, 2018.

24 Andrew Meola, "Distributed Ledger Technology & the Blockchain Explained," *Business Insider*, January 16, 2020.

25 Daniel Conte De Leon et al., "Blockchain: Properties and Misconceptions," *Asia Pacific Journal of Innovation and Entrepreneurship* 11, no. 3, April 2017.

26 Mike Orcutt, "How Secure Is Blockchain Really?" *MIT Technology Review*, April 2, 2020.

27 Brian Zambrano, "Blockchain Explained: How Does Immutability Work?" *VeryPossible*, February 27, 2018.

28 Computerphile, "Hashing Algorithms and Security—Computerphile," November 8, 2013, YouTube Video, 8:11.

29 Ed Featherston, "Blockchain: You Want Me to Trust a 'Trustless Trust' System?"

30 Matile, Raphael, and Christian Zurich, "Privacy, Verifiability, and Auditability in Blockchain-Based E-voting," *University of Zurich, Department of Informatics—Communication Systems Group*, April 4, 2018.

31 Christian Cachin and Marko Marko Vukolić, "Blockchain Consensus Protocols in the Wild," *Cornell University Computer Science*, July 7, 2017.

32 "How Many Businesses Accept Bitcoin? Full List (2020)," Fundera, January 1, 2020.

33 lbid.

34 Bernard Marr, "Bernard Marr & Co. Intelligent Business Performance," *Bernard Marr & Co, Intelligent Business Performance* (blog), August 2019.

35 Darcy W. E. Allen et al., "The Economics of Crypto-Democracy," *SSRN Electronic Journal*, 2017.

36 Shijie Zhang and Jong-Hyouk Lee, "Double-spending With a Sybil Attack in the Bitcoin Decentralized Network," *IEEE Transactions on Industrial Informatics* 15, no. 10, October 2019.

37 Daniel Krawisz, "The Proof-Of-Work Concept," *The Proof-of-Work Concept | Satoshi Nakamoto Institute*, June 24, 2013.

38 Julian Martinez, "Understanding Proof-Of-Work, Part 1: Demystifying Solving a Block," Medium, May 2018.

39 Gregory Trubetskoy, "Blockchain Proof-Of-Work Is a Decentralized Clock—Gregory Trubetskoy," *Gregory Trubetskoy* (blog), January 23, 2018.

40 Electronic Frontier Foundation SSD, "A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?" Surveillance Self-Defense, February 19, 2019.

41 Darrel R. Hankerson, Scott A. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, New York: Springer, 2011.

42 “Bitcoin n-Transactions-Total,” *Blockchain.com*, 2020.

43 lbid.

44 BitPay—April 16, “What Are Bitcoin Miner Fees?,” BitPay Support, April 2020.

45 Tushar, “How Many Transactions in One Block?” *Bitcoin Stack Exchange*, April 1, 2015.

46 Rahul Katarya and Aamir Mustafa, “Blockchain and Consensus Algorithms,” *SSRN Electronic Journal*, March 30, 2020.

CHAPTER 2

THE ECONOMICS OF VALUE

One day, a man went to an auction. When an exotic parrot went on the auction block, the man decided he was going to buy the bird no matter what. The bird was unbelievably rare, and he had been looking for this particular bird for an extraordinarily long time.

The man wanted the parrot so badly, he didn't think twice about the anonymous bidder who was consistently outbidding him. The man just kept bidding, getting outbid, and bidding higher and higher until he finally "won" the bird for a price of $23,000,000—a price the majority of auction investors would call "a definite bubble."

Despite his disappointment about the price, the beautiful bird was his at last.

As he was paying for the parrot, he said to the auctioneer, "I sure hope this parrot can talk. I would hate to have paid so much for it, only to discover that he can't speak!"

"Oh, don't you worry," said the auctioneer. "He's a talker. Who do you think kept bidding against you?"

PRICE AND VALUE

"Creating Value" is the corporate slogan of the twenty-first century. C-suite executives proudly parade around offering "value" at annual board meetings. Everyone seems to be obsessed with value, but no one seems to know precisely what it is. As with the man auctioning

for the parrot, a disconnect seems to exist between price and value, and within this gray area, a great deal of confusion and risk arises.

Value is not price. At best, price is a hazy reflection of value—our best attempt to collectively come to a flawed universal agreement on what it means to trade any given service or thing for an equal representation of the subcomponents of value (such as labor) in the form of currency. Prices are actually the **terms of exchange** that two parties engage with; this concept can get lost as transacting becomes so ingrained in us that we don't stop and think what price actually represents (a contract).

The whole system of valuation is shocking if you think about it. We have the ability to assign a price to an apple in relation to that of a multibillion-dollar behemoth such as Amazon. Society has the power to reflect the difference in how much we value one object/entity versus another. **That is not an arbitrary accomplishment at all. Currency is one of the most compelling human agreements and inventions.** Currency is the parameters we all agree to in order to make an exchange of value convenient for many.

Founder of the Austrian School of Economics Carl Menger was one of the greatest economists to tackle the ambiguity in "The Subjective Theory of value," written in the late 1800s.[47] He wrote, "When anything . . . whether of the material sort or not . . . **has both desiredness and scarcity, it then has value** for any person who concerns himself with it from this binary perspective."[48] Menger's theory follows that valuation for one person can look radically different from another. This isn't negative—a prevailing minority can believe in the desirableness of the underlying properties of an object, and that is all that truly matters for that object to be considered valuable. How much I value a paintbrush is going to look extremely different in relation to Picasso's valuation.

Menger's definition contrasts with other hazier, modern definitions, such as Huffington Post writer Caroline Banton's 2019 description of economic value as " . . . a measure of the benefit from a good or service to an economic agent. It is typically measured in units of currency. . . ."[49] Menger's definition isn't concerned about the benefit derived. Instead, his definition is purely focused on the individual's desire for what will be derived and how scarce the object of attention is. Banton's definition, which is widely visible on Investopedia for millions of eager students to read, is an example of how the definition of "value" has been watered down; the potency and specificity have drained away over time.

Where does the idea of intrinsic value fit into Menger's puzzle?

A house has "intrinsic value" for billions of people. Ask a group of intentional nomads how they value a house. What is the intrinsic value of a house for these nomads compared to you and me? Truthfully, a more accurate approach may be to view intrinsic value as a large number of people desiring underlying characteristics or function of an object such that the general consensus is that of readily agreed-upon value.

Intrinsic value is defined by the masses, creating generally agreed-upon prices. The masses can create uptrends in price and the masses also create downtrends as a result of the consensus of how desired the object is. As Menger stated, what the object is does not matter. The unprecedented truth that has altered the art of valuation is that in the twenty-first century, the rate and speed of information dispersal has increased drastically. The internet has quite literally made instant information a reality and as a result has allowed the masses' demand to shape-shift and form quicker than ever before.

If checks and balances weren't placed on the speed of this shape-shifting, we would begin to encounter ridiculous prices. For example,

during the COVID-19 pandemic, toilet paper was sold out in stores across the United States.[50] Hand sanitizer became a luxury. Clorox wipes were considered cleaning gold. If price gouging laws were not in place, you could have seen toilet paper worth ten to fifty dollars in some areas.[51] Enough people valued toilet paper during the crisis such that they prioritized it as a purchase before other items, and the speed at which this desirability valuation evolved ("hysteria," as the media would call it) happened exponentially faster than it would have happened half a century ago.

While the experts can calmly enter the marketplace and call the rest of the people sprinting to get toilet paper "irrational" because of their desire for what was perceived to be scarce toilet paper, at the end of the day, the masses and small sets of hoarders determined the shortage, not the armchair experts.

THE CURRENCY PROPOSITION

How does this circle back to cryptocurrency?

It all boils down to identifying the value of cryptocurrency.

Ameer Rosic, cofounder of BlockGeeks, defines cryptocurrency as "an internet-based medium of exchange which uses cryptographic functions to conduct financial transactions."[52] Any given cryptocurrency's worth is tied up in the trade of value between a buyer receiving a certain amount of cryptocurrency in exchange for a specified amount of currency the seller is demanding. While the US dollar is purely a medium of exchange, cryptocurrency (of which I will frequently interchange with "crypto" from now on) is special because not only is it a digital currency with a unique set of properties enabled by blockchain, but **crypto is also the means by which the underlying decentralized ledger is secured, maintained, and incentivized.**[53] Cryptocurrency unlocks certain

types of digital financial transactions that a US greenback cannot achieve on its own. Simply put, cryptocurrency has underlying utility that US greenbacks do not have.

"There are three eras of currency: commodity-based, politically-based, and now, math-based."

—CHRIS DIXON

Every blockchain enables different types of special financial transactions—the more valuable the transaction possibilities on any given blockchain, the greater the cryptocurrency will be priced because of the increase in desirability for that crypto's utility. This increased valuation happens because the cryptocurrency is both the facilitator and medium of exchange for these transactions on the blockchain ledger.

"Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us."[54]

—THOMAS CARPER, US SENATOR

While blockchain's reception has been overwhelmingly positive as a potentially valuable technology, the hegemony of sovereign currencies is uneasily facing the unprecedented competition presented by digital cryptocurrencies. The global hegemony understands digital cryptocurrencies have fundamental properties that are potentially more desirable than their paper currency alternatives. To return to where we began, **the value proposition of cryptocurrency may be stronger than traditional fiat; the consensus is still out.** A small tribe of individuals (compared to the stock market) have fiercely "speculated" and valued cryptocurrencies as being worth a significantly higher price than the majority of

people in the world.[55] Despite this, the intense desire for crypto by this small tribe of investors, against the better judgement of "experts," does not take away from the validity of what they are valuating. It merely increases the risk entailed by investing. The powerful investing institutions, miners, and retail investors will decide the degree to which these digital assets will be priced.

What is the value proposition of the dollar? To the left of the portrait of George Washington, the dollar proclaims: "This note is legal tender for all debts, public and private."

Hal R. Varian, a University of California Berkeley economist and *New York Times* columnist wrote, "A more profound, and perhaps slightly unsettling, reason that a dollar has value is simply that lots of people are willing to accept it as payment. In this view, the value of a dollar comes not so much from government mandate as from social convention."[56] This disturbing revelation reveals to us an unnerving truth: when a currency is purely a medium of exchange without utility, such as a piece of paper with ink on it, then the value of the dollar is purely built upon **trust** in the United States' ability to guarantee those dollars' transactional value. In addition, the purchasing power of any given dollar is based on the **scarcity** of the dollar—directly impacting the value as per Menger's model.

The **scarcity** of the dollar is wrapped up in the total amount of supply in circulation. Envision with me for a moment the following picture: you are staring at a swimming pool—the surface area of the water represents the supply of the dollar. The less surface area, or amount of dollars in circulation, for swimmers to swim around in, the more valuable every part of the pool is worth. You can fit more people in a pool than a hot tub, which is typically why the hot tub is going to be full more often than not; the small amount of room available in the hot tub makes it valuable compared to a spacious pool. Yet this

smaller surface area, corresponding to a smaller supply of dollars, is difficult to move around in, causing us to frequently bump into other people.

A mysterious entity called the Federal Reserve controls the size of the pool we all play in when it comes to the US dollar. As Roger Ver, a famous Bitcoin entrepreneur, put it: "At any time for any reason, the central banks can print as much money as they want. They call it things like quantitative easing . . . it makes the dollars you and I have worth less."[57] **The Federal Reserve are the pool designers, constantly increasing or decreasing the size of the pool at will.** This is where inflation created by the Federal Reserve deeply impacts the average person.

A simple thought experiment: how much is a dollar worth today compared to 1917?

Pause for a moment and genuinely make a guess.

The general belief is that the dollar is worth more now than it was back then. One dollar in 1913 had the same buying power as twenty-six dollars has in 2020.[58] This is a deceptive portrayal, so let me reframe.

Your one dollar today is only worth three cents in comparison to the dollar from 1913. The dollar has lost approximately 97 percent of its value because of inflation since 1913.[59] Not only is that ugly, it is downright terrifying.

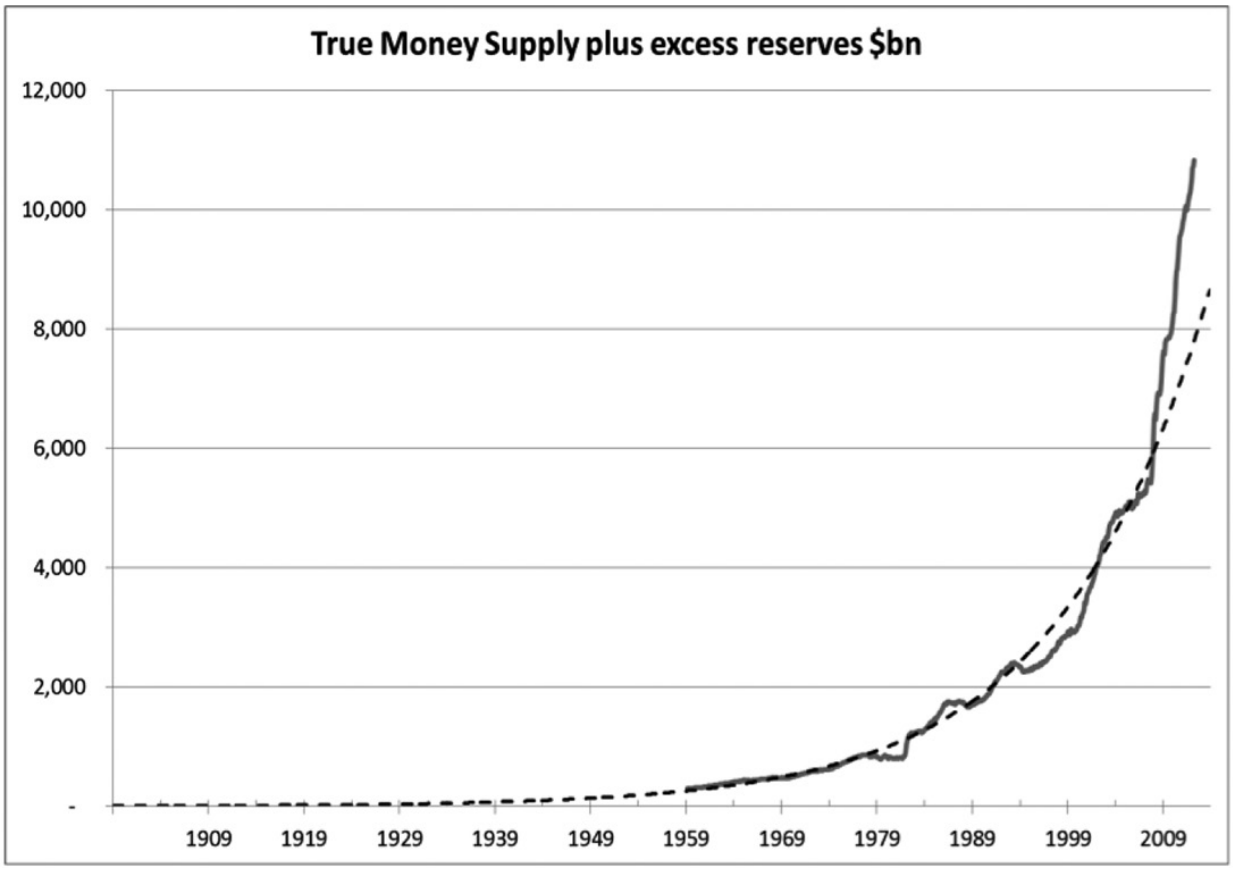


Figure 6: Money Supply[60]

The Federal Reserve has increased the size of the pool over time, and you can't blame them. More swimmers have entered the pool that need to trade and transact. But when the excess reserves grow faster than exponential growth (the dotted line), we have significant cause for concern.[61] Furthermore, this growth does not appear to be slowing down anytime soon. The Federal Reserve can choose to reduce the size of the pool, but it has refused to do so historically.

Why does the Federal Reserve refuse to reduce the size?

The Federal Reserve rents out the new pool space it creates to banks that then turn around and rent it out to swimmers, or everyday people and businesses, at a profit. Here is the catch: **the Federal Reserve can increase the size of the pool infinitely for free—simultaneously forcing a portion of everyone's dollar into the new pool space.** Printing money is free. Clever manipulation can

move the value of your dollars into the hands of those in cahoots with the banks and Federal Reserve, all without you doing anything.

And you can't stop it. Even members of the Federal Reserve understand this truth.

"Printing money doesn't produce goods and services. It doesn't hire people. It may seem like the right short-term medicine, but can the cure be worse than the disease?"[62]

—CHARLES PLOSSER, PRESIDENT OF THE FEDERAL RESERVE BANK OF PHILADELPHIA

THE ZIMBABWE STORY

Inflation is an ever-lurking danger. Zimbabwe has "trillion-dollar bills" worth pennies. Enter hyperinflation: the bane of a stable society.

"The Impact of Cryptocurrencies in Zimbabwe. An Analysis of Bitcoins," written by Anthony Tapiwa Mazikana in 2017, concluded that the Reserve Bank of Zimbabwe is hostile toward cryptocurrencies.[63] This is no surprise—no one wants to give up their control of the pool when it's a moneymaking machine and political tool. Yet the citizens of Zimbabwe appear to want to exit the murky monetary pool they swim in and move to the greener pastures of cryptocurrency.

Anita Posch, a podcaster and correspondent with CoinDesk, spent three weeks in Africa in February 2020 interviewing a variety of individuals about Bitcoin in Zimbabwe: "I wanted to see myself if this is true and how far Bitcoin is known and used there," she said in her podcast, "Bitcoin in Africa."[64] What motivated Anita to go on this unique trip? "Bitcoin is in my eyes first and foremost not a speculative, trading object, where everything is about price. For me it's a tool of liberation that enables individuals and communities to

free themselves of tight restrictions by authoritarian or totalitarian nation states that harm people's human rights."[65] Anita has pointed out that while first world countries go after cryptocurrency because of crime and lack of regulation, countries such as Zimbabwe must wage an all-out war against cryptocurrency because it would result in greater monetary freedom of citizens and a loss of power from the hands of the elite.

"Corruption is everywhere. And it seems that there are different rules for different people. Yes, I think one can say that for every country, but the differences are so big here. If you have USD, if you are in a high position, if you are in the right network, you can have a great life in Zimbabwe. I have seen private houses with swimming pools blue as the sky."[66]

—ANITA POSCH

Unfortunately for the majority of people in Zimbabwe, they are utterly tied down by the Zimbabwean dollar and monetary policy that cripple so many into abject poverty. When Anita asked an anonymous Zimbabwe online entrepreneur, "What do you think the use cases for Bitcoin are in Africa, or in Zimbabwe?" the anonymous entrepreneur was rather enthusiastic:

"If I can walk into the future . . . I see a lot of people actually taking the Bitcoin method . . . it's because of number one, our inflation rate . . . some people can actually use Bitcoin as a method to save money."[67]

The value of cryptocurrency is tied to guaranteed scarcity, lack of inflation, and the underlying desire for crypto's attributes.

But even amid the inflation and poverty in a country far away, the United States dollar reigns supreme as the determinant of wealth.

THE DOLLAR VERSUS CRYPTO

The primary factor that props up the dollar is the global agreement that the dollar is the de facto medium of exchange for the most valuable global transactions such as oil and other commodities. The dollar will continue to be so, enforced by the full might of the US government. And so we continue to trust it's plashing around in the pool without knowing where the edges of the pool are. We are not privy to that information.

This is where the value proposition of cryptocurrency becomes immediately apparent **purely from a scarcity perspective.** Using Bitcoin as our cryptocurrency example, there is a fixed number of Bitcoin: twenty-one million that will always exist.[68]

Not one more, not one less. No Central Reserve Bank. Cryptography and programming have been etched into the rules of the currency and the supplies. With Bitcoin, you know the size of the pool, and you never have to worry about your portion of the pool becoming less valuable because of inflation.

When we examine the **desiredness** of any currency, it always comes back to transparency and trust. The reason I will take cryptocurrency over a US dollar is because I trust mathematics and publicly visible monetary policies of a decentralized ledger more than the Federal Reserve. That isn't to say the Federal Reserve hasn't done a great job managing the US monetary policy and by extension the economy. It just means that people like you and me don't get to understand how many dollars are in circulation nor the justification for the strategies of the Federal Reserve. Instead, we are just along for the ride, hoping that the decision-makers behind closed doors won't take actions that damage the value of your dollar.

At the end of the day, I trust transparency more than anything, and I think most people do too. Because cryptocurrency is transparent in its design with monetary policy and circulation, I believe this will one

day make cryptocurrency increasingly more desired as a more trusted option versus traditional fiat currencies.

Not all cryptocurrencies have zero inflation. Some have planned inflation rates that are typically fixed, predictable, and notoriously difficult to change, which is usually a good thing. The monetary policy is voted for in a decentralized fashion and is entirely transparent. This is in stark contrast to a single centralized player determining the fate of everyone in the pool (looking at you, Federal Reserve).

Yet again, **welcome to a decentralized future.** And because Bitcoin is digital, it can split into much smaller denominators than one-one hundredth (good luck doing this to a greenback dollar beyond a hundred pennies).[69]

If the value of Bitcoin skyrockets, Bitcoin has the ability to be split into denominators as small as one hundred-millionth of a Bitcoin (also known as a "Sat," short for the creator of Bitcoin, Satoshi) to handle the full range of economic transactions.[70] This denomination splitting makes Bitcoin an extremely fluid currency. Note that the "splitting into smaller denominations" is not inflation; the boundaries of the pool remain firmly fixed. The pool is instead split up into smaller subplots to make it easier to have smaller transactions.

VALUE SPECULATION

What does it mean to speculate? As I think back to the COVID-19 pandemic, I begin to wonder who the speculators were. Are they the people who walked around without masks hugging other people until the last second before quarantine was declared? Are they the people who purchased apocalypse supplies long in advance? Or are they

armchair analysts who read the daily news and believed they had their finger on the pulse of society and reality?

Carter Thomas, a longtime investor in many different markets, has a quote that comes to mind for speculation: **"Reality is largely negotiable."** People will always have their theories and their stories—their triumphs and disasters. Interwoven between the present and the future are our speculations. Here is mine.

One day, we will live in a world where currency is decentralized, out of the control of any single entity. We will globally transact with people from all seven continents without needing multiple banks and intermediaries to conduct the transaction. Our exchanging of value will be peer to peer, person to person. Cryptocurrency will continue to be adopted because of its properties mentioned earlier in the book—**it's simply a better form of currency, even when you account for the trade-offs**. Blockchain technology will enable use cases that will shake centralized organizations to their core; entire businesses will be run in a decentralized fashion, with participants rewarded with cryptocurrency using an automated design. We will not use "banks" in the traditional sense—the blockchain and its universal ledger will be our futuristic bank. Some people, organizations, and countries will adapt. Some won't.

That is my reality, my negotiation with the future. Maybe I am an apocalyptic COVID-19 hoarder in a tribe of high-octane risk-takers investing in a speculative digital asset. I wouldn't say "maybe so"—it is definitely the truth. I don't deny it.

I want to be early to the game because great money has been made and is yet to be made by those willing to pull a chair up and believe collectively that **we are onto something here**, that this whole blockchain and cryptocurrency "thing" has potential to be seen as something with real intrinsic value.

Cryptocurrency is the very first instance of a currency capable of being decentralized, scarce, easily transportable, and digital. It is more reliably scarce than gold and more private and transactionally efficient than "modern" digital banking. This is why people are excited about cryptocurrency: it has the potential to completely and utterly revolutionize money, transactions, and contracts.

The game has changed drastically, and many are not aware of this new paradigm. Because of twenty-first century information transfer, cryptocurrency is **the first time a new form of currency can be this easily poured into and speculated in the long term outside of an individual's sovereign currency**. It is why those tied down in tough economic landscapes such as Zimbabwe are opening their arms to crypto. It is financial freedom guaranteed by mathematics and designed to resist the heaviest hitters in the world from shutting it down.

China has banned, unbanned, rebanned, and finally reopened the door for cryptocurrency effective January 1, 2020, with the passing of the Cryptography Law.[71] US regulators have uneasily begun outlining how to proceed with crypto regulation.[72] Warren Buffet has made comments concerning his thoughts on blockchain as an investment.[73] Clearly, the value of cryptocurrency and blockchain (which enables crypto) cannot be denied nor shut down any longer.

And yet painting a picture of an opportunity for easy money is far too easy. An abundance of writers, bloggers, and tweeters are peddling crypto investing as a walk through the park—an easy path to money. They encourage impulsiveness in the wrong way and push people to make atrocious financial decisions.

I am not here to do that. Do not mistake my enthusiasm for cryptocurrency and blockchain as a blind committal to throwing out logical investing principles to the wayside. **In reality, principles are**

all you have as an investor. Principles are the only thing you can truly control.

You now know what the cryptocurrency value thesis hinges upon and what it aims to solve. We explored value in tandem with price and how cryptocurrency is viewed under a traditional Austrian economics lens using scarcity and desiredness. In addition, we went after the US dollar and peeked behind the Federal Reserve vale of trust and inflation.

This chapter is an open invitation to temporarily explore a different pool other than the US currency pool you currently swim in. Instead, we will now dive into the stories of blockchain and cryptocurrency. How did this emerging technology come together?

---

47 Carl Menger, "The Subjective Theory of Value," *Innovator*, July 1967, Applications, Experiments, and Advanced Developments of Liberty edition.

48 lbid.

49 Caroline Banton, "The Definition of Economic Value," *Investopedia,* January 29, 2020.

50 Martinne Geller, "Toilet Paper Trophy Hunters on a Roll as U.S. Shortages Start Easing," *Reuters* (Thomson Reuters, April 29, 2020).

51 Baker Hostetler, "COVID-19 Update: Pricing during COVID-19 Without Gouging or Fixing," *JD Supra*, April 2020.

52 Ameer Rosic, "What Is Cryptocurrency? [Everything You Need To Know!]," Blockgeeks, May 5, 2020.

53 Reynold Stark, "Cryptoeconomics Vitalik Buterin—The Best Documentary Ever," December 5, 2017, Video, 54:23.

54 Senator Carper, "Chairman Carper Opening Statement at Senate Committee Hearing on Virtual Currency," November 18, 2013, Video, 10:40.

55 Annie, "Just 8 Percent of Americans Are Invested in Cryptocurrencies, Survey Says," CNBC, March 16, 2018.

56 Hal R. Varian, "Why Is That Dollar Bill in Your Pocket Worth Anything?," *The New York Times*, January 15, 2004.

57 *Bitcoin Documentary*, *Discovery Science Channel / Bitcoin Documentary*, 2017.

58 Kimberly Amadeo, "Why the Dollar Is Worth So Much Less Than It Used to Be," *The Balance,* April 13, 2020.

59 lbid.

60 Example 6: Courtesy of Goldmoney—Alasdair Macleod, "Gold versus the Money Supply," Goldmoney, October 10,2013.

61 Alasdair Macleod, "Gold-versus-the-Money-Supply," Goldmoney, accessed June 2, 2020.

62 Jim Bruce, "Money For Nothing—Inside the Federal Reserve," November 8, 2013, Video, 1:43.00.

63 Anthony Tapiwa Mazikana, "The Impact of Cryptocurrencies in Zimbabwe. An Analysis of Bitcoins," *SSRN Electronic Journal*, May 24, 2018.

64 Anita Posch, "Part 1 Zimbabwe: Ideal Conditions for Bitcoin?—Bitcoin in Africa: The Ubuntu Way," March 5, 2020, In Bitcoin Co Podcast, MP3 audio, 48:00.

65 Anita Posch, "Part 2 Living in a Multi-Currency World—Bitcoin in Africa: The Ubuntu Way," March 26, 2020, In Bitcoin Co Podcast, MP3 audio, 43:00.

66 Anita Posch, "Part 3: Using Bitcoin in Zimbabwe- Bitcoin in Africa: The Ubuntu Way," April 2, 2020, In Bitcoin Co Podcast, MP3 audio, 43:00.

67 lbid.

68 "Total-Bitcoins," Blockchain.com, Accessed June 2, 2020.

69 Ben Brown et al., "Bitcoin Units and Denominations: A Simple Breakdown From 1 BTC to 1 Satoshi," BlockExplorer News, September 19, 2018.

70 lbid.

71 Emily Parker, "Can China Contain Bitcoin?," MIT Technology Review (MIT Technology Review, April 2, 2020).

72 RBI, "US Lawmaker Introduces Crypto-Currency Act of 2020 While Under Coronavirus Quarantine: Regulation Bitcoin News," Bitcoin News, March 10, 2020.

73 Satoshi, "Warren Buffett Slates Bitcoin, Denies Owning Crypto Gifted by Justin Sun: Featured Bitcoin News," Bitcoin News, February 24, 2020.

CHAPTER 3

DIGITAL PIONEERS—THE STORIES OF DECENTRALIZATION

Any groundbreaking technology "stands on the shoulders of giants." This is true for the capital investment, the risks, the failures, and the successes of those who have gone before. In software development, individuals use the libraries and platforms of others to build their own creations: tools built on top of tools built on tools from tools. It is tools all the way down. Somewhere along the way were the ideators: those who had a vision of "what could be" long before anyone else did. They saw the potential for horizontal integration into a countless number of industries. They built the tools that could usurp centralized behemoths that have existed for an eternity. They set out into the unknown. These are their stories.

THE INVENTOR OF BLOCKCHAIN

Long before the Satoshi Nakamotos, the Vitalik Buterins, and the Brian Behlendorfs of the world was a humble professor from Berkeley named David Chaum.[74] Called by some "The Forefather of Cryptocurrencies and the Cyperphunk Movement," David was the first to set out to research the possibility of designing a computation protocol that could be trusted by mutually distrustful parties.[75] The research of this problem occurred from the late 1970s to the early 1980s. The backdrop of this research was at the University of California, Berkeley, a long-standing key player in cryptographic research and other computer security-related projects. His research

occurred at a time when researchers from Berkeley were arrested for trying to get the newly-created and highly valuable Rivest-Shamir-Adleman algorithm smuggled across the US-Mexico border. The military complex was the backdrop of much of the research at the time—of which many "cyberpunks" at Berkeley were not a fan of.

According to Dr. Chaum, "If you can solve the trust problem, you can solve any information security problem."[76] The dissertation he completed offered up a potential protocol solution to the trust problem, which **included every element of a blockchain that Bitcoin has—except proof-of-work.** The fact that proof-of-work was not included in Dr. Chaum's dissertation makes perfectly good sense. The idea of burning up tons of computing time in the early 1980s in order for consensus to be reached within a blockchain protocol would have been considered entirely unreasonable and unfeasible.[77] In addition, his paper "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" was not digitized until much later in time:

"It's a little bit ironic, I guess, that my concern about digital sovereignty and all made me not sign the copyright of my dissertation over to something called 'dissertation abstracts' that, like most theses, would be online and you could find them and order copies. So, I kept the copyright of everything. It just basically lived in the library in paper form. There were only three copies in three different parts of the library system, but never digitized."[78]

—DAVID CHAUM

Dr. Chaum recounted in an interview with *Epicenter Podcast* how the three copies were nearly constantly checked out for long periods of time. It was a "best-kept secret" in many ways—something Chaum regretted later as his dissertation did not garner the credit it may

have received if he had placed the dissertation into online circulation.

Since his dissertation, Dr. Chaum has been credited as the inventor or contributor to research on secure digital cash, cryptographic blind signatures, digital group signatures, trustworthy voting systems, an anonymous credential system, zero-knowledge arguments, and zero-knowledge proofs. He is quite the accomplished researcher. Dr. Chaum believes the "killer app for consumers" is messaging integrated with payments hosted on a blockchain with privacy fully integrated.[79]

"Privacy is tied intimately to human potential."

—DAVID CHAUM

For Dr. Chaum, his current project is to make this killer app a reality through Elixxer. It aims to be the communications layer of the "xx network," protecting privacy by combining end-to-end encryption with an accelerated mix network that obscures metadata generated by a user's daily activities.[80] Dr. Chaum is not done as a digital pioneer yet. As he continues to be a leader in the privacy and cryptography space, there is no telling what is around the corner with him.

THE ANONYMOUS CREATOR

Satoshi Nakamoto.

The name evokes a sense of mystery. **With a market cap of $300 billion, Bitcoin and its creator to this day remain anonymous.** No one knows who created Bitcoin except the creator. This is unprecedented in human history and is part of the draw for many in the Bitcoin community.[81]

In 2008, a website called bitcoin.org was launched. This was during a troubled time—the 2008 financial crisis saw the birth of the Occupy Wall Street movement and the creation of groups such as Anonymous.[82] Self-proclaimed libertarian ideologies expanded rapidly during a time when financial freedom was seemingly entirely within the hands of the central banks and their decisions. Over nine million Americans lost their jobs during the crisis and the monetary system that had been steady for so long was now in jeopardy.[83] On September 15, 2008, the 158-year-old Wall Street investment bank Lehman Brothers filed for bankruptcy.[84] Online forums that had fallen silent in the early 2000s centered around the idea of creating a global currency outside of the modern-day banking system roared back to life after the financial crisis.[85]

On October 31, 2008, shortly after the bankruptcy was announced, the white paper for Bitcoin was published to a cryptography mailing. The so-called "Satoshi Nakamato" proclaimed the following: "I've developed a new open-source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on cryptography proof instead of trust."[86]

What was the inspiration for this innovation? Whoever Satoshi Nakamoto is was clearly inspired by the problems brought to the forefront in 2008.

"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. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."[87]

—SATOSHI NAKAMATO

From white paper to reality, on January 3, 2009, Satoshi Nakamoto revealed thirty thousand lines of code that were the birth of Bitcoin. The codebase for Bitcoin to this day is publicly visible and hosted on GitHub, using Git software to provide codebase management.[88] January 3, 2009, was the day the Bitcoin blockchain network had its first block ("Block 0") mined. This was done by Hal Finney, an early fan and developer of Bitcoin, working in conjunction with the mysterious and anonymous Satoshi Nakamoto.

The message inserted into Block 0 that is fittingly embedded into Bitcoin's ledger forever into perpetuity was as follows: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"—a reference to the broken banking system.[89]

Interestingly enough, Hal Finney was one of the few individuals to consistently have message chains with Satoshi. Evidently, Satoshi ignored any questions concerning the identity of who was behind the mask of "Satoshi Nakamoto."

"I thought I was dealing with a young man of Japanese ancestry who was very smart and sincere. I've had the good fortune to know many brilliant people over the course of my life, so I recognize the signs."

—HAL FINNEY

A small group of merchants made it possible to purchase items using Bitcoin. Laszlo Hanyecz, widely known as the "Bitcoin Pizza Guy" became the first person to use Bitcoin to purchase goods—two pizzas for ten thousand BTC in May 2010.[90] At the all-time high price for Bitcoin, those pizzas would have been worth $200 million. Despite this tragedy, only when digital pioneers such as Laszlo started utilizing Bitcoin for its intended purpose did Bitcoin eventually achieve the high value it holds today.

Hundreds of developers still build on the Bitcoin blockchain to this day. At the very beginning of Bitcoin, Satoshi Nakamoto had 100 percent control of the code base and was the only person capable of proposing and pushing out actual quality-of-life code changes to Bitcoin's protocol. Gavin Andresen was one of the few hyperactive developers who worked indirectly with Satoshi Nakamoto on the Bitcoin protocol development. In mid-2010, Satoshi Nakamoto updated bitcoin.org and removed his email from the website. This left Gavin Andresen as the only publicly-facing individual whom news organizations, questions, and developers could reach out to.

On April 27, 2011, Gavin Andresen announced he would be attending an emerging technology conference set to be hosted at the CIA headquarters in Langley, Virginia.[91] Four days before Gavin tweeted to the general community concerning this meetup, Satoshi Nakamoto emailed Mike Hearn (a former Google employee and active developer and contributor to Bitcoin) with the following: "I've moved on to other things. It's in good hands with [Andresen] and everyone." This was Satoshi Nakamoto's last contact with the Bitcoin project in any capacity. Many speculate Gavin's contact with the CIA was what pushed Satoshi to completely disappear. Satoshi's final act was ceding control of the codebase to Gavin, who then

shared control with four other well-known developers in the community to carry the torch.

Since Satoshi Nakamoto's vanishing act, Bitcoin code updates are pushed out by Bitcoin Improvement Proposals (BIPs).[92] Over three hundred BIPs have been proposed, many of which sit in limbo as the community reviews them to make sure they align with the protocol's original goals as outlined by Satoshi's white paper.[93] Bitcoin has, to date, over five hundred million transactions.[94] Satoshi's vision of a decentralized future is steadily being realized. We will only ever be able to imagine who Satoshi is.

"If you don't believe it or don't get it, I don't have the time to try to convince you, sorry."

—SATOSHI NAKAMOTO (ONLINE FORUM POST)

THE FACE OF DECENTRALIZATION

Separate from the mysterious intrigue surrounding Satoshi is a young man who was inspired by giants such as Satoshi and Dr. Chaum. Meet Vitalik Buterin, a twenty-six-year-old Russian Canadian college dropout who created the Ethereum blockchain protocol. With over 105,000 software developers building or experimenting on the Ethereum blockchain, Vitalik Buterin may have been the spark that lit the adoption of applications built on blockchain.[95]

Vitalik Buterin was born January 31, 1994, in Kolomna, Russia, to Dmitry Buterin (a computer scientist) and Natalia Ameline.[96] At the age of six, his family immigrated to Canada for better job prospects. In third grade, Vitalik was placed in an accelerated learning path where he focused on math, programming, and economics. He

attended a renowned private high school in Toronto called the Abelard School for his high school years. When Vitalik was seventeen, he learned about something called "Bitcoin" from his father. Vitalik wrote it off initially because "it didn't seem like it had any intrinsic value." Apparently, Vitalik heard about Bitcoin again, and this time it piqued his interest to investigate a little bit deeper. Vitalik wrote articles for 5 BTC per article. Using this all but worthless Bitcoin (at the time), he was able to interact with the Bitcoin decentralized ledger.[97] His initial interest started with currency, but it eventually shifted to economics and the political implications of what Bitcoin could do.

In late 2013 on a trip to Israel, Vitalik encountered a blockchain community that was focused on building applications other than currency on top of blockchain technology. In Israel, MasterCoin was attempting the very first protocols that would enable financial contracts and cryptocurrencies issued from a blockchain. Vitalik observed much of what the teams were trying to accomplish with their programming had redundancy and could be replaced by a new programming language as a means for more efficient use case creation.[98]

Over the course of the next couple of months, Vitalik went about creating Solidity, the native smart contract coding language of the Ethereum blockchain. As Vitalik began to innovate this new language, he began to understand that what Satoshi Nakamoto had enabled was a new paradigm. The foundation Satoshi had established led Vitalik to the realization that "you can do a lot more with cryptographic systems if you simultaneously view them as economic systems."[99]

Can decentralization be the basis for the next generations of phone apps, websites, and services you use? Vitalik believes so. He believes

the development of the Ethereum blockchain was part of "creating the floodgate of decentralization."

"When I came up with Ethereum, my first thought was, 'Okay, this thing is too good to be true.' As it turned out, the core Ethereum idea was good—fundamentally, completely sound."[100]

—VITALIK BUTERIN

How did Vitalik open the floodgate? What is Ethereum capable of that Bitcoin is not? Bitcoin by design has every transaction verified and processed by every node within the Bitcoin network. With over 10,600 nodes as part of the Bitcoin network, **the network is only as fast as the weakest link.**[101] If a complex program is run on the Bitcoin protocol, the entire network would grind to a halt until the weakest node computes the problem. Bitcoin avoids this problem using a fee system based on transaction size. This makes highly complex programs impossibly expensive to post to the blockchain ledger. This work around is clever but leaves Bitcoin with the problem of being classified as Turing Incomplete—a lack of guarantee that any given program will be completed.[102]

Vitalik made great progress solving this Bitcoin design flaw within the design of Ethereum by creating a system of "gas" and the Ethereum Virtual Machine (EVM). The EVM is a virtual computer hosted on the distributed ledger—a brilliant concept that allows for everyone to use a globally visible and distributed computer that anyone can access and use if they pay a fee in gas. The entries on a ledger are essentially "blocks of memory" that, just as with a normal computer, can be manipulated to perform decentralized computations, allowing for the creation of decentralized apps, or Dapps, which are outside of the control of any single authority.

What problem is Vitalik trying to solve today? Currently, Ethereum is faced with the problem of **scalability.**[103] Visa is able to update and manage over 1,700 transactions per second using its centralized servers.[104] That's quite impressive. PayPal handles about two hundred transactions per second.[105] All of these centralized companies are in stark contrast to the decentralized computation capabilities of Ethereum, which is only able to process **twenty-five transactions per second.**[106]

This is the most important fundamental problem that remains to be solved by Vitalik and the Ethereum developer community. The faster the network, the more complex the types of Dapps can be hosted and used by everyday people. Scalability also enables users to be able to send cryptocurrency (in this case, Ether) much quicker between each other. Speed is clearly valued in the twenty-first century.

"Scalability is this idea of coming up with a blockchain that can scale much larger than existing chains essentially by processing transactions in parallel. And moving away from this paradigm where every single node on the network has to process every single transaction."

—VITALIK BUTERIN

Vitalik, with the help of developers working on the "Casper" chain of Ethereum, have proposed a solution to scalability known as "sharding." Sharding aims to split the ledger into different pieces (that still remain connected), allowing for different shards of the ledger to be appended and updated by different sets of nodes.[107] This makes the verification system faster by removing the constraint of needing every single node to verify every single transaction of the ledger. Unfortunately, the trade-off the protocol encounters while

implementing sharding is that the decentralized network becomes **less secure.**

At most, a decentralized protocol can only implement two of the following properties to the fullest: decentralization, security, or scalability. This was dubbed by Vitalik as the "scalability problem," which is a permanent limitation and side effect of blockchain design.[108]

Perhaps harder than the "scalability problem" is trust; Vitalik acknowledges it is the most difficult problem to solve for emerging technologies such as blockchain.

"The main advantage of blockchain technology is supposed to be that it's more secure, but new technologies are generally hard for people to trust, and this paradox can't really be avoided."

—VITALIK BUTERIN

THE BRIDGE BUILDER

How do I get my money from cash into cryptocurrency? How do you do it legally? How do you do it quickly? What services are trusted by regulators?

At the inception of cryptocurrency back in 2008, no simple way of trading sovereign currency for cryptocurrency existed. An exchange is what allows people to trade one currency for another (in this case USD for cryptocurrency). In order for an exchange to work, it must have a working relationship with both banks and the government—a monumental task indeed.

Jed McCaleb was the original founder and programmer of the online Bitcoin exchange, Mt. Gox. It was the largest Bitcoin exchange in early 2014, accounting for over 70 percent of all Bitcoin

transactions. When McCaleb first started the exchange in early 2010, he didn't think much of it. He just wanted to have a way to quickly transact with other people. In fact, the name "Mt. Gox" was an old domain name he reused from his earlier days where he had created a *Magic: The Gathering* card exchange.

"Mt. Gox was just kind of on a lark almost just because I wanted to learn more about the, like how Bitcoin works and this is just a good way to learn about the system. So it wasn't like it was ever intended to be like this massive business or anything like this."[109]

—JED MCCALEB

Jed originally designed the exchange to use PayPal as an on-ramp from fiat to crypto. This lasted four months, until PayPal banned Mt. Gox (and McCaleb) for life because of charge-back fraud from a variety of accounts interacting with Mt. Gox.[110] Because of the rapid growth of Mt. Gox from zero users to a couple of thousand, an overwhelmed Jed sold Mt. Gox to Mark Karpeles, a French entrepreneur, for an insignificant amount. This sale turned Mt. Gox into a Japanese exchange—the beginning of the end of the largest Bitcoin exchange.

Months after the sale, Mt. Gox had a flash crash occur that saw the price of Bitcoin on the exchange drop from seventeen dollars to a couple of cents in a matter of seconds.[111] The exploit "compromised a user account" and stole twenty-five thousand Bitcoin from customers on the exchange, which was worth $8.5 million at the time. A string of breaches, regulatory problems, and US government run-ins impacted Mt. Gox from 2011 to 2013. A $75 million lawsuit with CoinLab, a partner with Mt. Gox, worried customers because of the allegation that Mt. Gox "willfully failed to perform its obligations."[112] Five million dollars were taken by the US government

because Mt. Gox operated "without a license to transmit money."[113] Customers suffered from withdrawal problems, causing justified panic as people began to exit the exchange.

In early February 2014, Karpeles revealed a hacker had slowly been draining the exchange of Bitcoin using an undiscovered exploit. Over 740,000 Bitcoin had been stolen from users over time (roughly $14.8 billion at Bitcoin's all time high).[114] On February 28, 2014, Mt. Gox filed for bankruptcy.[115] Over 24,750 claims worth $432 million were approved on May 25, 2016.[116] This concluded Mt. Gox and what was once the largest Bitcoin exchange.

With this utter collapse, many had questions about what a successful exchange would look like. What would bring people to an exchange in the long term? How do you survive all the problems an exchange incurs?

An exchange ultimately needed to be extremely secure, easy to use, fully compliant with the law, and communicative with customers. This is where Brian Armstrong, founder of Coinbase, entered the picture.

"At Coinbase, our first priority is to ensure that we operate the most secure and compliant digital currency exchange in the world."

—BRIAN ARMSTRONG

Valued at over $8 billion as of 2018, Coinbase was created in 2012 in the wake of Mt. Gox. Brian Armstrong had learned early on that the key to long term success for an exchange would be built upon working directly with regulators. Coinbase applied for a money transmitter license in 2013 (unlike Mt. Gox).[117] Ramping up the number of employees quickly, Coinbase has over a thousand employees today. Hiring elite software engineers, Coinbase,

"through a combination of luck and skill" (according to Brian), managed to front run many of the best hackers circling a variety of crypto exchanges.

"When I was thinking about starting Coinbase, a few people told me I was crazy to try creating a custodial crypto wallet and exchange. The best hackers in the world were trying to break into crypto exchanges, and Mt. Gox along with many others had suffered breaches. . . . Coinbase managed to weather the barrage of attacks, and created many novel methods of [private] key storage"[118]

—BRIAN ARMSTRONG

With a clean user interface, excellent customer support, and a variety of initiatives in the space, Brian Armstrong has turned Coinbase from a small exchange into an industry titan. Coinbase has done over $2 billion in volume traded in a single day, and has over twenty-eight cryptocurrencies available for purchase, sale, and transfer.[119] Coinbase has undeniably played a key role in allowing for the adoption of cryptocurrency by opening the channel of exchange between sovereign currencies and cryptocurrencies with legally compliant and safe procedures for investors.

Brian, as with many of the pioneers of the decentralized movement, is a firm believer that cryptocurrency and blockchain will soon be embedded in society.

"I think it's going to end up a lot like the internet. Some countries try to regulate the internet—Bitcoin will be very much like that. It will be legal, and there will be some countries with currency control."

—BRIAN ARMSTRONG

There are countless stories of those who have contributed to blockchain in the last decade. Their stories are numerous, but David

Chaum, Satoshi Nakamoto, Vitalik Buterin, and Brian Armstrong were the integral players along the way who enabled the technology, development, and adoption of decentralized ledger technology. They were the ideators, the ones who saw and took a risk on a future no one else envisioned. Without them, we would not have landed on the proverbial moon. Many cryptocurrencies have blown up, imploded, copied, recycled, raised money, and fallen away into obscurity.

Regardless, everyone learning about this technology domain is a pioneer. **You are a pioneer.** And as blockchain emerges into the public eye, we must never forget the stories told and untold that have made blockchain and cryptocurrency possible.

---

74 Nathaniel Popper, "The People Leading the Blockchain Revolution," The New York Times (The New York Times, June 28, 2018).

75 Epicenter Podcast, "David Chaum: The Forefather of Cryptocurrencies and the Cypherpunk Movement (#304)," September 10, 2019, Video, 1:03.57.

76 lbid.

77 lbid.

78 lbid.

79 Distributed, "Distributed 2018: Keynote Presentation—David Chaum," August 20, 2018, Video, 25:01.

80 "The Decentralized Dream, Realized," Elixxir, accessed June 2, 2020.

81 Alex Lielacher, "Why Has Satoshi Nakamoto Remained Anonymous?" Brave New Coin, April 15, 2018.

82 Joanna Walters, "Occupy America: Protests against Wall Street and Inequality Hit 70 Cities," The Guardian (Guardian News and Media, October 8, 2011).

83 Tommy Andres, "Divided Decade: How the Financial Crisis Changed Jobs," Marketplace, April 29, 2019.

84 David Floyd, "10 Years After Lehman: Bitcoin and Wall Street Are Closer Than Ever," CoinDesk (CoinDesk, September 13, 2018).

85 Zoë Bernard, "Everything You Need to Know about Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of Its Creator," *Business Insider,* (Business Insider, November 10, 2018).

86 Satoshi Nakamoto, "Bitcoin Open Source Implementation of P2P Currency: Satoshi Nakamoto Institute," Bitcoin open source implementation of P2P currency | Satoshi Nakamoto Institute, February 11, 2009.

87 Ibid.

88 Bitcoin, "Bitcoin Github Repository," GitHub, June 1, 2020.

89 David Floyd, "Genesis Block: Chancellor on Brink of Second Bailout for Banks · Monnos," Monnos, April 15, 2020.

90 Galen Moore, "10 Years On, Laszlo Hanyecz Has No Regrets About His $45M Bitcoin Pizzas," CoinDesk (CoinDesk, May 22, 2020).

91 David Canellis. "Satoshi Nakamoto Left Bitcoin Because of the CIA, a Theory," Hard Fork | The Next Web, July 19, 2019.

92 Sfox, "Bitcoin Governance: What Are BIPs and How Do They Work?," SFOX Edge, April 16, 2019.

93 Ibid.

94 "Bitcoin n-Transactions-Total," Blockchain.com, 2020.

95 Paybis, "How Many Blockchain Developers Are There In 2020?" Paybis Blog, May 18, 2020.

96 Morgan Peck, "The Uncanny Mind That Built Ethereum," *Wired* (Conde Nast, June 16, 2017).

97 Ibid.

98 Michael Noel, "Vitalik Buterin The Boy Genius Behind Ethereum," November 8, 2017, Video, 59:55.

99 Ibid.

100 Ibid.

101 "Global Bitcoin Nodes Distribution," Bitnodes, June 2, 2020.

102 Kyle Wang, "Ethereum: Turing-Completeness and Rich Statefulness Explained," *Hacker Noon*, June 1, 2020.

103 Kenny Li, "The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed," Hacker Noon, June 1, 2020.

104 lbid.

105 Daniela Mechkaroska and Aleksandra Popovska-Mitrovikj, "Analysis of the Possibilities for Improvement of BlockChain Technology," *Telecommunications Forum (TELFOR)*, November 26, 2018.

106 lbid.

107 "Ethereum Sharding Explained: Understanding Ethereum," district0x Education Portal, Accessed June 1, 2018.

108 Toju Ometoruwa , "Solving the Blockchain Trilemma: Decentralization, Security & Scalability," *Coin Bureau*, June 12, 2018.

109 Adrianne Jeffries, "Inside the Bizarre Upside-down Bankruptcy of Mt. Gox," *The Verge,* March 22, 2018.

110 James Noah, "Mt. Gox Interviews: Jed McCaleb on the Creation of Mt. Gox," Hacker Noon, February 26, 2019.

111 Andrew Norry, "The History of the Mt Gox Hack: Bitcoin's Biggest Heist," Blockonomi, March 31, 2020.

112 Adrian Chen, "Massive Bitcoin Business Partnership Devolves Into $75 Million Lawsuit," *Gawker*, May 2, 2013.

113 Declan McCullagh, "Homeland Security Cuts off Dwolla Bitcoin Transfers," *CNET*, May 14, 2013.

114 Nathaniel Popper, "How Mt. Gox Imploded," *Vice*, May 19, 2015.

115 lbid.

116 lbid.

117 Brian Armstrong, "What Happened in Crypto over the Last Decade," *Medium, The Coinbase Blog*, March 5, 2020.

118 lbid.

119 Danny Nelson and Nikhilesh De, "Coinbase Broke Traffic Records and Saw Massive Volume During Market Collapse," CoinDesk, March 20, 2020.

CHAPTER 4

USE CASES—SYNERGY & FINAL FRONTIERS

Understanding how a Swiss Army knife opens and closes is not nearly as captivating as watching one in action. For the average person going about their day, understanding how the internet works is last on their list of things to do compared to watching another episode of *Friends* or the next March Madness basketball game. This is the beauty of technology that fundamentally changes the world—what it enables becomes far more important than how the technology works. We are tool-using creatures. Kids can navigate an iPad at the age of four. A curious individual can know the temperature outside by glancing at a piece of glass and circuits. Millions of people type on little plastic shapes that darken and lighten pixels on a screen that are then perceived as letters and symbols. You make phone calls at the touch of a button without stopping and pondering just how incredible it all is. And yet somehow we navigate the digital world *intuitively*. Isn't it all just a little absurd?

The use cases of blockchain are vast, ambitious, and utterly mind boggling. Valuable characteristics of a blockchain are as follows: decentralization, transparency, and immutability. We have discussed blockchain and the digital currency it enables, but what other mechanisms can be baked into the blockchain ledger itself? The most important mechanism enabled is a **smart contract.**[120]

You can picture a smart contract as a vending machine (albeit a digital one).[121] People approach the vending machine and insert currency into the machine. The machine makes it perfectly clear that if you hit "A5," you are going to receive a bag of Cheetos. In addition,

you know exactly where the destination for what you are receiving is going to be—right at the bottom of the machine. The process is clear as day, simplistic, and largely self evident.

A smart contract is just that—**a vending machine hosted on the blockchain.** Smart contracts have public addresses, just like anyone who owns any cryptocurrency of a particular blockchain. Anyone can interact with the digital vending machine (smart contract) by sending cryptocurrency to the public address of the smart contract. The smart contract will then execute autonomously and spit back out the digital equivalent of a bag of Cheetos based on how that particular vending machine is designed. **Note that the design of smart contracts is publicly visible and, once committed to the blockchain, immutable—no one can tamper or change that particular vending machine once it's hosted on the blockchain, just like how transactions are immutable once appended to the ledger.** This is what enables so called "trustless trust" when it comes to digital contracts.

Smart contracts are where a large amount of the utility of blockchains is from—they are a perfectly neutral third party in the form of a program. Why interact with a Cheetos salesman in person if you can just use a vending machine that will guarantee the entire exchange will be fair? What smart contracts are capable of achieving are only limited by creativity and implementation. Implementation of smart contracts is tied to a simple question: **How can we replace a human intermediary with the digital vending machine equivalent?**

SIMPLE SMART CONTRACTS

Today is your first day of work. The year is 2030. Your employer asks for your public crypto wallet address. Your employer then posts a

smart contract on the blockchain that interacts with the company's wallet—designed such that the digital vending machine (smart contract) pays you two ETH (a cryptocurrency) every five days for the next two months. This smart contract is perfectly automated, out of the hands of any third party once it is posted. The HR team no longer has to worry about posting or managing this payment process once the smart contract is set up, saving time and money. In addition, as a worker you are happy because the whole process, once posted, is immutable. Your contract is locked in and guaranteed, and you no longer are in the hands of a human party.

Andrew walks up to a voting booth, and casts a ballot (digital or physical, it does not matter). After Andrew casts his ballot, a nefarious actor changes his vote. Andrew is angry, how is it possible for a vote to be changed?

The government decides to modernize. The new voting infrastructure implements a blockchain. The "voting" smart contract hosted on the blockchain would receive votes as inputs, updating the total for candidate A and candidate B. At the end of the allotted time, a single token is automatically sent to the public address that represents the winning candidate. The best part? **Because transactions on a blockchain are guaranteed to be immutable, your vote can never be changed.** The history and decision of each vote is etched into the history of the ledger. Cryptographically, the election is secure.

You are in your late twenties and finally decide to purchase a house. Your friend Carol has posted a smart contract on the blockchain that transfers ownership of the deed over to the buyer, along with a seller's affidavit that will be appended to the blockchain permanently —notarizing the purchase in perpetuity in the name of the buyer. The contract is publicly visible, so you are able to make sure you want to partake in the transaction.

You decide to buy the house for the listed contract amount. You send ten Bitcoin to this smart contract, and the entire exchange between you and Carol is automatically executed. Carol receives her Bitcoin for the house, and you publicly own the property through the passing of the documents digitally through the blockchain. No lawyers, brokers, or third parties. The entire transaction was peer to peer and significantly cheaper than the current series of hoops you must jump through to buy and sell a house.

INDUSTRY INTEGRATION

While there are many hypothetical examples that we can think of that could benefit from this technology, what truly matters are the industries being directly impacted. The following is a list of the most important industries looking to implement blockchain—and, by extension, smart contracts. Sometimes the revolution is a shared ledger, and other times it is simply the use of smart contracts. The following is an impacted industry list endorsed by ConsenSys, a market leading blockchain technology company.[122]

- Health Care
- Banking & Finance
- Digital Identity
- Energy & Sustainability
- Government and the Public Sector
- International Trade & Commodities
- Law
- Media & Entertainment
- Real Estate
- Supply Chain
- Digital Assets

This is a jaw-dropping list. Most new technologies only have the ability to impact a few industries, but blockchain, as a trusted ledger, opens up the door to horizontal integration possibilities in a variety of value chains within a wide range of industries. Horizontal integration is when integration occurs between multiple systems or companies that are on the same "layer" of the value chain.

As we begin to dive into the use cases in each category, I would encourage you to imagine the possibilities of tomorrow. For you pessimists, never forget that even the original creators of great technologies have been overly bearish and conservative in what could be.

"I think there is a world market for maybe five computers."

—THOMAS J. WATSON, CHAIRMAN OF IBM, 1943

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

—CLIFFORD STOLL, 1995

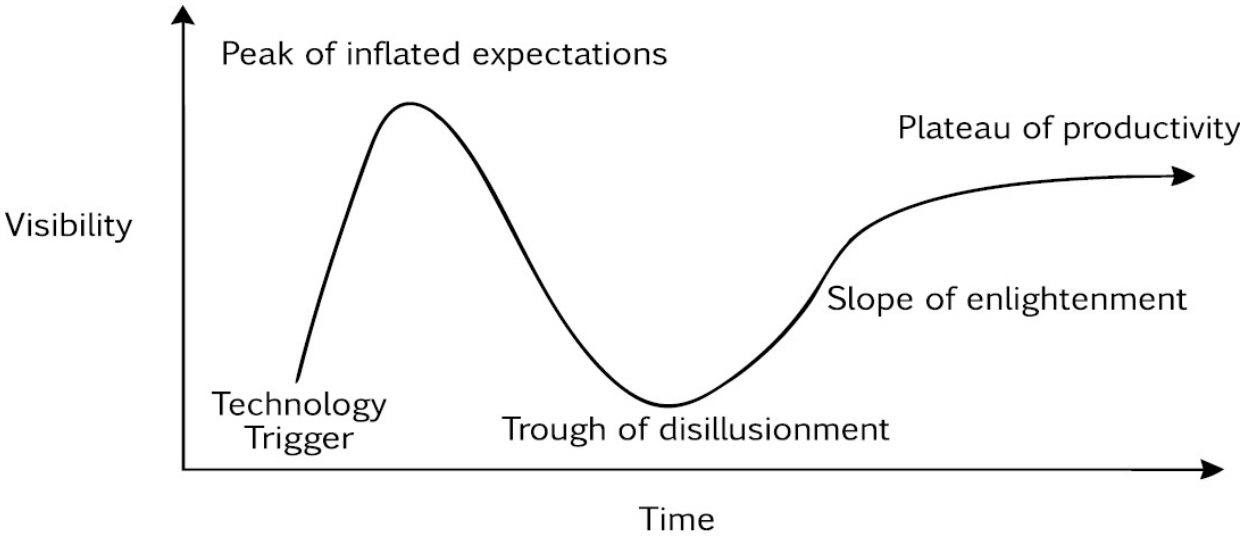


Figure 7: Gartner Hype Cycle

Pessimism is a natural response to innovation when the speed of progress does not meet the unbridled enthusiasm of speculation and expectation. Your job as an investor or user of blockchain technology is to find the legitimate and significant use cases only blockchain can solve. Never lose sight of the fact that blockchain is a decentralized ledger that mutually distrustful parties can trust.

HEALTH CARE

Hospitals and the health care system are notorious for slow horizontal integration.[123] To this day, some hospitals still keep records in paper form. Sometimes, this is the only form of record keeping. Antiquated systems of record keeping leave patient data scattered across a variety of mediums and locations. **No universal patient identifier exists.** This leaves hospitals juggling information between each other, creating data mismatches and errors. The problem of sharing records and verifying the validity of an individual in a system is costly. Interoperability is defined as the way different health care providers are able to share, search, and query medical records.

According to Shaun Grannis (director of the Center for Biomedical Informatics):

*"Statistics show that up to **one in five** patient records are not accurately matched even within the same health-care system. As many as **half** of the patient records are mismatched when data is transferred between health-care systems."*[124]

This is utterly shocking. The customer is stuck with long phone calls and larger bills because of these types of issues—entirely unaware of this type of fundamental communication problem that exists within health care systems. Not only is it costly, it can hurt patients if wrong treatments are applied.

Information blocking, the restraint on the exchange of patient information, is the next issue.[125] Hospitals do this because they do not want to lose patients—there exists monetary incentive for many third parties working in parallel to the hospital systems for this to be true. Ever wondered why having providers work with a variety of hospitals for a single patient is so difficult? Information blocking is a core problem.

How can blockchain solve information blocking and data mismatches? **Imagine a world where all health care providers and hospitals use the same digital ledger of data**. This ledger would be—you guessed it—a blockchain. This immediately solves the problem of data mismatches; everyone would be referencing the same set of data. Hospitals would benefit because of reduced labor costs of dealing with data mismatches, patients would have better health care, and communication/update of patient records would be instant and universally shared.

" Our current health ecosystem consists of a plethora of disparate IT legacy systems that have been amassed over the years that do not

communicate well with each other. Blockchain would provide the ability to replace these disparate systems with a single system that offers interoperability."[126]

—DAVID RANDALL, PRADEEP GOEL, RAMZI ABUJAMRA

Instead of hospitals, insurance companies, and third-party IT companies owning your data, **you would have control over who gets access to your health data**. Your private keys, which are used to sign transactions on the blockchain, would be the only way to unlock your encrypted health care data. Only through permitted use of your keys could someone alter, view, or "delete" your data. The public key that everyone is able to see and interact with would be your **universal patient identifier**, verified by your private key that only you have access to. This is unbelievably powerful—you would own your health care identity instead of having fragments of your identity flung between multiple different parties without your knowledge or consent.

Currently, you have to make ten to twenty calls to different doctors and providers who cross-check information records and prior conditions, all while navigating health care bureaucracy and policy. **With one unified blockchain ledger, those hoops simply disappear** with the horizontal integration benefits blockchain provides. You would be able to easily interact with smart contracts (picture them as apps on your phone) that are hosted on the health care blockchain and would instantly check if you are qualified for certain programs, benefits, or plans. A smart contract (vending machine) hosted on the blockchain would be able to objectively (with your permission) check your data to see if you apply to any of the previously listed health care opportunities—all without a third party involved.

A health care blockchain also enables **data backups**.[127] Currently, each hospital and provider must back up its own data. With blockchain, everyone has the identical "ledger" of data, creating a valuable safety net of redundancy. In addition, the chain of records that intrinsically makes a blockchain what it is creates an **immutable audit trail for everyone to view**. Gone would be the days of paper record confusion or disparate digital records in conflict with each other. Disputes would be reduced to "who made this change?" as opposed to "which change is correct out of these multiple records?" The singular, universal blockchain ledger will play an integral part in the path to better health care for everyone. And to think that this only scratches the surface of all the different blockchain applications in health care!

"Blockchain distributed ledger technology can advance the biomedical and health care domains in various novel ways, and we expect many new applications to emerge soon."[128]

—JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION

BANKING & FINANCE PROBLEMS

The modern-day consumer lives in a world of continuity—we want frictionless transactions. We have enough hassles currently, which is why I think we can all agree we want banking to be easy. Consumers and businesses want loans to be simple. Terms of use *should* be clear as day: "I don't have time to navigate all the red tape." For most people, a large portion of their banking experience has an acceptable amount of friction. I mean, the system does work, doesn't it? I can swipe my card at Cub Foods, Venmo seems smooth, and paying off loans is *relatively straightforward.*

Unquestionably, we have grown up to accept the quirks of working with monolithic banks and companies of tremendous scale. This way

of life thus begs the question: “Why are banks as large as they are? What product am I being sold? What is the cost?” This is the beauty of the bells and whistles of our finance system as we know it.

It all works.

But the reason it works is because you the consumer, investor, and trader pay hidden fees. We pay for the cost of trust and the cost of interoperability between a variety of parties that make the full nine yards of financial instruments possible. The interchange of property is where the money is earned and the cost delegated in hushed contractual terms.

“If commentators and students of the US banking system could be said to agree on any single point, it would be that the system now in place is absurdly complex and inefficient.”

—CARTER GOLEMBE

Where in particular are the costs incurred in our finance system?

“The duplicate and time-consuming post-trade processes that banks, brokerages, custodians and clearing houses undertake to reconcile multiple ledgers represent a very large cost of trust embedded in the existing system.”[129]

—CENTER OF ECONOMIC POLICY RESEARCH

Notice costs incurred are related to the different parties reconciling their own *separate* ledgers. Translation: reconciling distrust between two ledgers is expensive.

Another problem everyday businesses face is generating capital through either a business loan (banking capital) or venture capital. Banks and venture capitalists turn a profit in the safest possible manner with the highest possible risk/reward obtainable. The

problem with these capital loaning entities is that many businesses with brilliant ideas and potential enterprises are barred from raising capital for their business because of third-party credit verification, required track records of past successes, absurdly high interest rates, and subjective valuations impacting terms and conditions in an unfavorable manner.

On the other side of this problem are **individuals** who are not accredited venture capitalists.[130] You and I are blocked from being able to invest in some of the most lucrative investments on the planet because of "investor safety red tape," which is essentially legislation that "protects" average consumers from investing in high-risk enterprises.[131] While this is understandable, the freedom to use your money how you want is in many ways an expression of your freedom of speech. You should have the right to invest in the same opportunities wealthy individuals have access to.

Cross-border payments are expensive and slow not only for citizens but also for banks. This is because of banks relying on "Nostro" accounts, which is essentially a bank's account within another bank that is used for transactions between the two banks.[132] Oftentimes, currency exchanges occur between two different currencies—introducing liquidity problems and exchange rate conflicts on top of standard liquidity problems (Bank A needs x amount of capital from Bank B, but Bank B can only provide half of what Bank A wants). Ultimately, the additional intermediation layers increase complexity, counterparty risks, and cost for all parties.

Remittance fees grew to $600 billion in 2018.[133] Rates have stabilized around 7.5 percent—an extremely lucrative profitability point for banks.[134] The problem for individuals is somewhere along the value chain a bank is involved, and because of Know Your Customer standards and government legislation, millions of people

globally are trapped into paying high rates to simply transfer value across borders between countries.

Securities and derivatives clearing and settlement globally are executed nearly instantly. Unfortunately, the clearing and settlement of transactions can take one to three days. Worse, derivatives can take weeks to even years to settle depending on the complexity of the contract. The derivatives market is estimated to be holding over $1.2 quadrillion worth of the world's value.[135] That is ten times more than the total world GDP locked up in inefficient settling and transferring of value in the current securities and derivatives settlement system.

It would appear distrust is costly.

THE DEFI SOLUTION

Blockchain and finance are like bread and butter—they just make sense. So much so that a new term has been birthed: DeFi, or decentralized finance. DeFi is the ecosystem of financial applications (digital vending machines concerned with finance) that are built on top of blockchain in the form of smart contracts. Hundreds of smart contracts can interact with each other, allowing for completely automated and decentralized exchanges, derivatives markets, and tokenization platforms. DeFi is the solution to all the problems previously listed. Let us return to our very first problem of raising capital.

When new companies or networks utilize an initial coin offering, or **ICO**, many individual investors, who do not have the capital to be venture capitalists or bankers, suddenly have the ability to invest directly into ownership of a business or a new digital asset. An ICO is simply a smart contract (remember the vending machine analogy) that exchanges one cryptocurrency for another (although there have been plenty of USD for cryptocurrency ICOs). Anyone can raise

capital by publishing their own ICO smart contract, and anyone can be a venture capitalist (without all the red tape) by sending cryptocurrency to a digital vending machine (smart contract). This solves the first two problems described—the ability to raise money as well as the ability to be your own venture capitalist without accreditation.

Nearly $5.6 billion was raised through ICOs alone in 2017, creating quite a bit of commotion in the finance world.[136] Needless to say, blockchain's ability to reliably funnel investment capital into startups is inspiring and will continue to be one of the primary use cases.

Solving the cross-border payment problem has already been solved with blockchain technology. Anyone with an internet connection and a cryptocurrency wallet can send their token of choice to any other public wallet in the world: **no banks involved, no third parties, and no geographical restrictions.** Fees are as low as ten cents for any amount of capital sent, which is to say that you could send a billion dollars' worth of Bitcoin and the transaction fee would only cost ten cents.

A survey by Clovr found that 15.8 percent of individuals surveyed globally used cryptocurrency as opposed to traditional remittance options.[137] This number will continue to increase as accessibility, adoption, and education increase globally surrounding cryptocurrencies. The properties of cryptocurrency enabled by a variety of blockchain protocols are trailblazing the new standard for currencies. While many would stand in the path of radical technology, history has proven humanity will choose the better product if given the choice.

"Bitcoin, and the ideas behind it, will be a disrupter to the traditional notions of currency. In the end, currency will be better for it."

—EDMUND MOY, THIRTY-EIGHTH DIRECTOR OF THE UNITED STATES MINT

The Ripple transaction protocol (RTXP) is attempting to unify banks around the world using blockchain—**solving "Nostro" account transaction friction.** Today over a hundred financial institutions are on the Ripple blockchain network, including Standard Chartered Bank, Westpac, Banco Santander, and BBVA.[138] Using a series of private blockchains unified under one global ledger, Ripple is capable of assisting in the transfer of billions of dollars' worth of value on a daily basis, with transactions taking less than four seconds, compared to the traditional three to five days. While Ripple is considered "centralized" by decentralized standards, it is representative of an important undertow: banks are now willing to work with blockchain projects.

"For Ripple, the global liquidity problem is measured in the trillions of dollars, I think that people are realizing that Ripple is gaining traction, we're gaining engagement, we're gaining more customers. So there's been interest in that."[139]

—BRAD GARLINGHOUSE, CEO OF RIPPLE

Finally, the **securities and derivatives challenge** is being addressed by the NASDAQ. Working in tandem with Chain and a variety of other startups, the NASDAQ is actively experimenting with new infrastructure that would be an improvement on outdated transaction frameworks.

Digital Asset Holdings is a financial technology company that builds products (built on top of blockchains) for regulated financial market infrastructure providers such as banks, exchanges, and custodians. Digital Asset Holdings is working with ASX (Australian Stock Exchange) to completely replace the current clearing and settlement infrastructure with a ledger-based solution that is permissioned in nature.[140] In many ways, if this application can be achieved, the final frontier of settlements would be on the horizon.

"I had seen the financial crisis unfold, and I had seen the credit derivatives market get operationally ahead of itself, which resulted in systemic risk counter-party exposures. I began to believe that distributed ledgers had the capability to tackle that problem."[141]

—BLYTHE MASTERS, FORMER EXECUTIVE AT JPMORGAN CHASE

DIGITAL IDENTITY

Rarely do we notice the role of identity until it is questioned.

Identity is who you are as a unique individual, how you are represented, and how you are allowed to interact. According to a frequently-quoted study by Microsoft, online users have, on average, the following: twenty-five accounts, six and a half passwords (shared across 3.9 different sites), with an average entry of eight passwords per day.[142] **Your ability to interact with the digital world and the real world is tied to your ability to prove who you are.** This is a messy process that has been smoothed over to the point of being bearable in some moments, and terribly inconvenient in others (I'm looking at you, DMV).

First, let's break down the current process. Your physical attributes (name, age, gender, address, birthplace, biometrics, etc.) are tied to a physical document, with a stamp of approval from a sovereign

authority that essentially says, "Yeah, this person now exists according to us, and this person is unique from someone else for the following reasons . . ." For Americans, this is the Social Security Number. The SSN is the basis for a swath of critical interactions. Other physical instruments such as a driver's license or passport are created and verified based on the verification of the "key" social security number. These "layer two" documents are created are then used in a variety of interactions for either payments (such as banks needing to know who you are), permissions (can't join the military without proper verification of who you are), and participation (this concert only allows people twenty-one and above).

Identity theft was called "crime of the new millennium" by the assistant US Attorney in 2001.[143] The prediction stood the test of time: identity theft impacted 14,400,000 Americans in 2018, worth $1.5 billion in out-of-pocket costs alone (not accounting for the true economic loss of resolving these incidents).[144] The first six months of 2019 had seen 3,800 publicly-disclosed breaches, not accounting for unreported hacks. **A whopping 4,100,000,000 records were compromised, of which 65 percent pertained to passwords and identity.**[145] These are devastating statistics. What were the core contributors?

1. Centralized Data Management
2. Scattered Identity
3. Identity Redundancy

THE FUTURE OF IDENTITY

Imagine for a moment you walk into a store. We will call it "Century Groceries." The first time you enter the store, you fill out a form for the manager. You are given a copy of this form. A week later, you come back to Century Groceries and are barred from entry unless you

can produce the form. Frustrated, you head over to Bob's Burgers where the same process is rinsed and repeated. Deep within the basement of Century Groceries is a stack of thousands of forms that were filled out. These forms have to be pulled out and cross-checked with a customer's form every time one tries to walk in the door. Over at Bob's Burgers, someone breaks into the basement and grabs the form you registered with Bob's Burgers. They walk straight into Century Groceries because you used the same form for entry into both.

What you have here is an imperfect representation of the internet as we know it today.

The internet's slipshod "solution" to digital identity is deeply flawed. Every website is its own stand-alone bastion of verification—all based on a flawed username/password system. The system is inconvenient, insecure, and downright tedious. We should follow a similar model to that of the real world, where core documents verify "layer two" documents that would make your life easier to navigate the digital world.

This is where blockchain enters as quite literally a "key" solution. An identity blockchain solution such as SelfKey (a $22,000,000 ICO in 2018) proposed the following series of steps as a solution.[146] First, you create a digital wallet or have one issued to you by the government. This wallet will hold all your key digital documents on your local device. Next, a private key and public key are generated inside of the wallet. At this point in time, you are the only party that knows this particular private key. It is 100 percent unique to you as a user. It's the digital equivalent of your thumbprint or retina. The private key is what is used to verify and authenticate a variety of third parties attempting to confirm you are in fact you. This works because **the unique combination of your exact private key in**

combination with the public key allows third parties to verify the authenticity of the wallet and its owner without being able to know what the private key is. It'd be like if you mashed together your Social Security Number with your first and last name to produce something that could only be made by you—and was universally recognized by the rest of the world as being you.

This unique public key that represents you as a unique user is what is hosted on the blockchain. It's the shortcut that allows you to walk into the digital equivalent of Century Groceries and immediately into Bob's Burgers without needing to pull out forms from the basement. In fact, these stores do not even need to store or protect forms anymore!

Everyone using the digital management blockchain would share the same ledger of public keys that represent unique people with unique private keys, allowing them to seamlessly traverse the web.

The cryptography that enables the key exchanges between two parties without revealing the underlying private keys is called the **Diffie-Hellman key exchange.** Mathematically, this algorithm is beautiful. If you have the time, there are amazing explanations that do not include math and instead describe it using buckets of paint and color mixing.[147] Diffie-Hellman key exchange enables PKI (Public Key Infrastructure), the foundation of the internet's functionality.

In the future, your public key will exist on a blockchain. In combination with your private key stored in your digital wallet, you will be able to create and gather digital identity instruments into your digital wallet that will allow you to seamlessly navigate the web without needing burdensome passwords and usernames, just like the real world. Even better, in this new system, your private key and critical digital documents are not exposed or sitting in hundreds of data silos. The whole system is safer, quicker, and built on a

mathematical system of trust. Minimal information is shared, and you have ultimate control over your digital identity. Personally, I look forward to the day when I don't have to enter in a username or password on a website to verify I am in fact who I say I am on the web.

"Current identity systems are limiting Fintech innovation as well as secure and efficient service delivery in Financial Services and society more broadly. Digital identity is widely recognized as the next step in identity systems."[148]

—WORLD ECONOMIC FORUM

The list of blockchain use cases and applications are limitless. The synergy between our current working world with the attributes enabled by blockchain will change our society as we know it. Readily accessible digital vending machines (smart contracts) for all sorts of transactions are a replacement for many antiquated systems. Decentralized ledgers put distrustful parties on the same page using a perfectly neutral and auditable party because of the nature of a decentralized ledger. The possibilities are exciting, and I would encourage you to continue to explore the vast number of ways blockchain is changing the future of our tomorrow.

---

120 BitDegree, "What Is a Smart Contract and How Do Smart Contracts Work," *BitDegree*, January 21, 2020.

121 Nick Szabo, "The Idea Of Smart Contracts," *Nick Szabo*, accessed June 2, 2020.

122 "Blockchain Use Cases in 2020: Real World Industry Applications," *ConsenSys*, accessed June 1, 2019.

123 Blockgeeks, "Real World Blockchain Applications—Healthcare," February 22, 2019, 5:04.

124 Kate Monica, "Regenstrief to Develop Automated Patient EHR Matching Solution," EHRIntelligence, August 14, 2017.

125 Kurt Jensen, "More Data More Problems: Fixing EHRs and Information Blocking in Healthcare," Health Professions Network, February 20, 2020.

126 David Randall, Pradeep Goel, and Ramzi Abujamra, "Blockchain Applications and Use Cases in Health Information Technology," *Journal of Health & Medical Informatics* 08, no. 03 (2017).

127 lbid.

128 Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications," *Journal of the American Medical Informatics Association* 24, no. 6 (August 2017).

129 M., Casey, J. Crane, G. Gensler, S. Johnson and N. Narula, "The Impact of Blockchain Technology and Finance: A Catalyst for Change," *Geneva Report on the World Economy No. 21*, 2018.

130 Eva Su, "Accredited Investor Definition and Private Securities Markets," Accredited investor definition and private securities markets § (n.d.))

131 "Venture Capital Vs Business Loans: A Beginner's Guide to Financing Alternatives," Business Funding, Working Capital Loans, Small Business Loans, March 13, 2019.

132 "Nostro Account—Overview, How It Works, Example.,"Corporate Finance Institute, Accessed June 2, 2020.

133 Steve Cecchetti and Kim Schoenholtz, "The Stubbornly High Cost of Remittances," *Money, Banking and Financial Markets* February 19, 2018.

134 lbid.

135 Peter Cohan, "Big Risk: $1.2 Quadrillion Derivatives Market Dwarfs World GDP," AOL, July 15, 2016.

136 "Only 48% of ICOs Were Successful Last Year—but Startups Still Managed to Raise $5.6 Billion | Currency News | Financial and Business News | Markets Insider," Business Insider, Accessed June 2, 2020.

137 "Sending Money Back Home," Clovr, February 24, 2020.

138 Alex Moskov, "What Is Ripple (XRP)?: A Complete Guide to the Banking Cryptocurrency," CoinCentral, May 29, 2020.

139 Molly Jane Zuckerman, "Ripple CEO Talks Liquidity And Regulation: Ultimately Governments Aren't Going Away," Cointelegraph, March 6, 2018.

140 Maria Nikolova, "ASX Takes Its Investment in Digital Asset to $30.9m," FinanceFeeds, December 13, 2019.

141 Edward Robinson and Matthew Leising, "Blythe Masters Tells Banks the Blockchain Changes Everything," Bloomberg.com, September 1, 2015.

142 Shirley Kennedy, "Your Password Has Expired and Must Be Changed," *Information Today, Inc.*, April 2016.

143 Sean Hoar, "Identity Theft: The Crime of the New Millennium," *HeinOnline*, 2001.

144 Insurance Information Institute, "Facts Statistics: Identity Theft and Cybercrime," *III*, January 2018.

145 lbid.

146 SelfKey Foundation, "Self Key," (Whitepaper, September 11, 2017).

147 Art of the Problem, "Public key cryptography—Diffie-Hellman Key Exchange (full version)," July 30, 2012, Video, 8:37.

148 Lyndel Melrose, "A Blueprint for Digital Identity: Deloitte Papua New Guinea: Financial Services," Deloitte Australia, November 7, 2017.

CHAPTER 5

ON LOSS AND HOW IT HAPPENS

"Failure is so important. We speak about success all the time. It is the ability to resist failure or use failure that often leads to greater success."

—J.K. Rowling

We cannot deny the fact that you can lose money. The world is built upon the success of many, and on the surface of financial success, we almost never see the statistics for failure. Traditionally, the majority of writers appear to have an unspoken social contract to only talk about what creates success. I am going to buck that right off the bat by having a whole chapter devoted to losing and failing with investing.

The stories of failure are countless, and most go untold.

Rob P. Gekwiak is a rare counterexample, in his single video recounting his story of failure.[149] Rob speaks about it as if he is talking about the loss of a loved one—a trace of sadness and tension clearly resides on his face and in his tone as he begins his story: *"I didn't really want to put this out, but I know people support me no matter what."* He takes a deep breath in, and then continues, *"I put all of my money into crypto and then some . . . I was just over everything. I thought I could see this trend happening—so I started putting all of my money into crypto."* He made the veritable first mistake so many do: overleveraging what they own on the roll of a die. This quiet, unfounded belief that they can beat the market throws them into treacherous water.

What is heartbreaking about Rob is thousands of people are just like him, but few are brave enough to embrace it and issue a warning to others. *"I just said f*ck it. I had this really YOLO mentality. I thought to myself, 'If the gain is a hundred times then it's worth it for losing ten times. Well guess what happened? The loss was ten times. Money I didn't have that I owed on bills I put into crypto."* Hindsight is twenty-

twenty for winners and losers. But some losses are more likely than others, and people such as Rob are aware of this after the fact. *"I made a ridiculous decision, and it destroyed me."*

Others have slightly different stories, ones of rags to riches, and then back to rags again. *"I refused to sell . . . such a stupid move man . . . such a stupid move."* Meet Simon Golestan, founder of Advertisely. Simon's story started in 2017 with investing in Bitcoin when it was worth $7,000 after talking to his friend Nick at an In-N-Out Burger joint. After reinvesting his money into Vechain (another cryptocurrency), his crypto net worth grew to $337,000. During the crash of 2018, instead of exiting while he was profitable, Simon continued to hold on as Vechain lost nearly 97 percent of its value. *"Why sell? I believed it would come back up. But it never did. It literally never went back up. I said to myself, 'I will let it go to zero instead, I refuse to sell.'"* In the end, Simon sold all of his cryptocurrency for $20,000. He walked away better than most because of how early he got it in, but clearly he learned some harsh lessons.

Unfortunately, Simon took his YouTube investment confessional down in early 2020—whether it was shame, embarrassment, or simply looking for a fresh start, he was not open to commenting.

THE RSM TITANIC AND RESPONSIBILITY

When the RSM Titanic was launched in 1911, the world believed it had found an unstoppable beast. It was the second of three Olympic-class ocean liners, seemingly impeccable in design. *"I cannot imagine any condition which would cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel. Modern ship building has gone beyond that."*[150] Captain Smith was the commander of the Titanic, an experienced veteran with over forty years of sailing experience. The Titanic is fraught with many valuable lessons, but

the most important elements were never of the ship itself. The factor that was not accounted for by Captain Smith was that of human error and confidence.

"I thought her unsinkable and I based my opinion on the best expert advice."[151]

—PHILLIP FRANKLIN, WHITE STAR LINE VICE PRESIDENT

You would think someone like Philip Franklin to be the expert; the person who is a straight shooter and expert in the Titanic industry. But he wasn't. Any expert that is trying to sell you on the idea that something has a guarantee of success is a wolf. There is no sheep's clothing involved. They are the easiest to spot. Visible at the frontline shouting about their success, even as they try to sell you a spot on the lifeboat they are exiting onto. A great deal of failure is bound up in a deadly human bias. **Just because someone knows more than you on an investment does not mean their knowledge or thesis is correct.** Traditionally, the unassuming builders, designers, and veteran users are where the truth resides.

"Let the Truth be known, no ship is unsinkable. The bigger the ship, the easier it is to sink her. I learned long ago that if you design how a ship'll sink, you can keep her afloat. I proposed all the watertight compartments and the double hull to slow these ships from sinking. In that way, you get everyone off. There's time for help to arrive . . ."[152]

—THOMAS ANDREWS, MANAGING DIRECTOR OF HARLAND AND WOLFF SHIPYARDS

Clearly a disconnect existed between the people who make the boats and the people who sell the boats. This is the first lesson of loss: **you have the responsibility to decide who you listen to and trust.** Peter Lynch, a legendary Wall Street investor who produced 29.2 percent annualized return for thirteen years, put it pointedly: *"There seems to be an unwritten rule on Wall Street. If you don't understand it,*

then put your life savings into it." Lack of education is a lurking killer. Until you understand what you are investing in as well as the likelihood that investment is to fail, then you will be someone who fails to accept that your investment is sinking until it is all the way under the water.

As Eva Hart, a titanic survivor, put it, *"And it wasn't until we were in the lifeboat and rowing away, it wasn't until then I realized that ship's going to sink. It hits me there."*[153] Eva Hart is our example of a hopeless speculator, someone who couldn't accept a loss until it was too late. It's okay to take a loss. I would never recommend anyone to invest unless they have the ability to accept a loss. Investors that are not capable of this are usually one of three things: **prideful, ill prepared, or greedy.**

You will notice thus far that many of the factors of loss are controllable and yet deeply interwoven into human nature. I myself was in a similar situation. When Ethereum (the cryptocurrency I was invested in) skyrocketed from $400 to $1400 in 2018, I was stuffed with pride. I was brimming with confidence that I had made an investment of a lifetime. I didn't have a strategy or an exit plan. **I was the trifecta of perfect sins, emboldened by the adrenaline of seeing so much success so quickly.** I was in every way no different than Simon Golestan, caught up in the excitement of the moment.

"When arranging a tour around the United States I had decided to cross on the Titanic. It was rather a novelty to be on the largest ship yet launched. It was no exaggeration to say that it was quite easy to lose one's way on such a ship."[154]

—LAWRENCE BEESLEY, TITANIC SURVIVOR

I was lost on that proverbial ship and I learned a lesson I would never forget. If you fail to plan your buying and selling strategy you face the

possibility of losing money. Anyone can tell you this. But what is the deeper lesson? What do you learn when you get lost on the ship and finally find your way out? For me it was this: **If you fail to actively plan against your lowest human instincts, then you face the guarantee of deep investment regret.** Investment wisdom isn't cheap and it often has a price tag known as "a big mistake" attached to it. The sooner you take responsibility for the levity of your own decisions, the sooner you will be on a path that veers away from failure.

"The most important quality for an investor is temperament, not intellect."

—WARREN BUFFETT

THE BUFFALO CYCLE

Success with investing is an iceberg—beneath it lies the skeletons of those who fell to the wayside from fear, lack of patience, mistiming, emotional investing, irresponsible loans, and (perhaps the most dangerous) ignorance. Are these preventable? What do we control? Fear. Uncertainty. Doubt. Despair? The big drop. The free fall. Portfolio in the red. Fifty straight days of percentage losses. That stomach-emptying feeling. The sadness. The hopelessness. When you invest in crypto without principles, these moments will throw you around. Because cryptocurrency is more volatile than any traditional investment, herd investors are regularly eaten up by the wolves of volatility. With or without a plan, crypto investing is not for the faint of heart. If your conviction cannot look at some level of "danger" in the eye and see opportunity, then you may consider investing in a US T-bill, which offers a "wild" 2 percent return on your fifty-two-week investment.

Hey, no judgement—some people enjoy watching paint dry.

The key to avoiding failure consistently is to have firm principles. It lies entirely within your hands how much time you put into researching which cryptocurrencies and investments you are putting your money into. Every investor has agency, and you must have principles to guide your agency. Some investors might not feel that they have the choice every moment, but you always have control over when you buy and sell. You control how much belief you have in the future of any investment. This book has an entire chapter devoted to principles—suffice it to say they are a patchwork solution to human behavior.

The beauty of having investment principles is you give yourself the chance to be ahead of the herd. You get to gracefully exit when things get scary because the writing will be on the wall. Humans are pack animals that repeatedly fall prey to the cycles of tribalistic mindsets. "Safety in numbers" until those numbers lead you astray. **When you run with the buffalo, you lose track of where the cliff is.** The alternative? Track the pack, follow it, but never get sucked into the madness of euphoria.

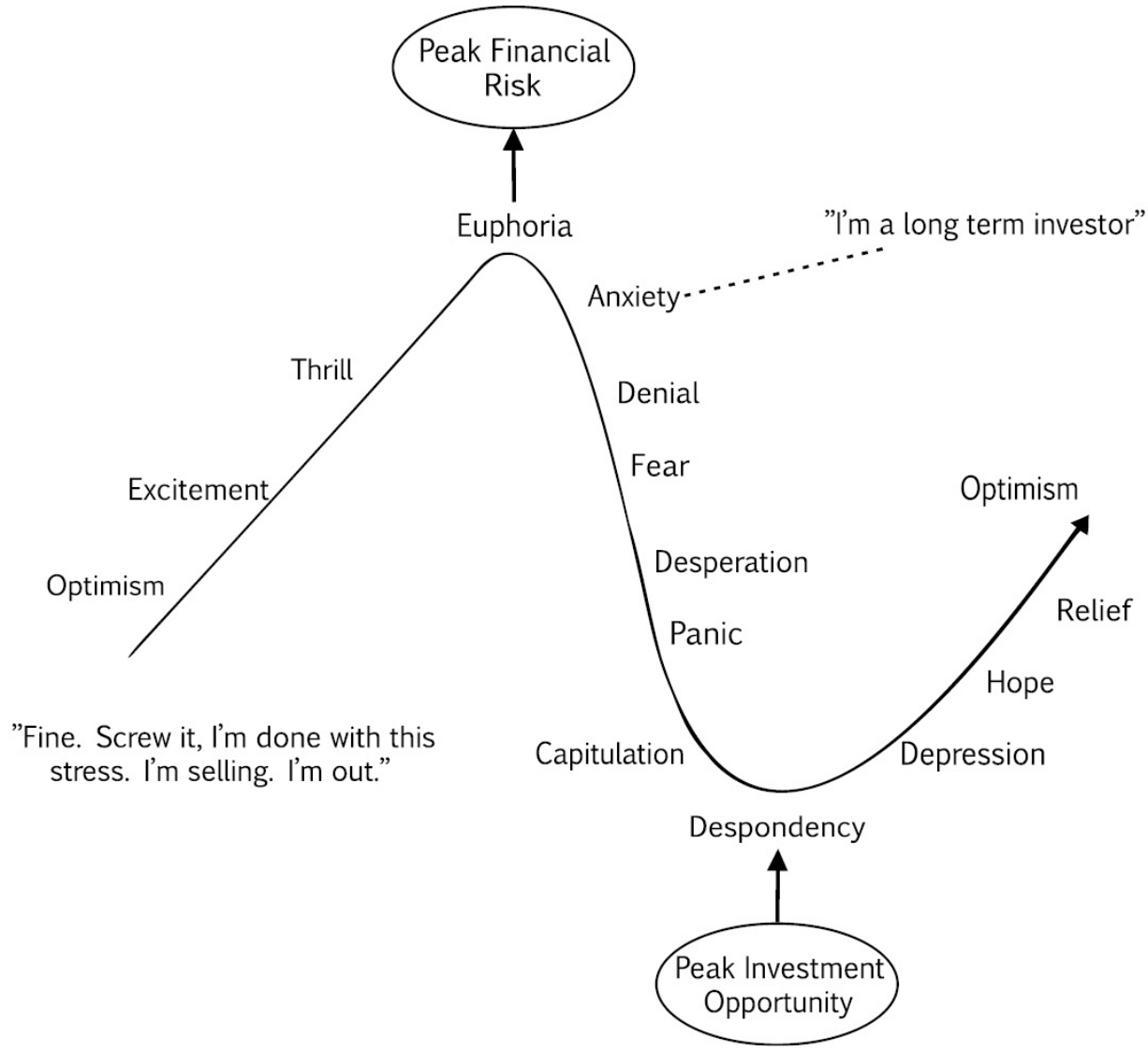


Image 9: Investment Hype Cycle

The online places we go to for opinion, advice, and comfort during drops or upward climbs in price can turn us into herd animals. YouTube, Facebook, Twitter, Reddit, Instagram, and texting can all lead to amplified emotions. This fogs our ability to understand the fundamentals we are investing in, often causing a hasty, fear-filled decision to buy and sell. Suddenly, you get this "sense" everyone is investing in something else and you need to do it right now: the Buffalo Cycle. It is vicious and it is everywhere. Investors without a plan and without principles are pulled along the emotional roller-

coaster. These investors are brought to the edge of euphoria and thrown off into the valley of despondency. Most investors understand these cycles, but to be able to act on any of these trends is difficult, the key is to avoid denial. **Stay realistic and stay humble.**

At the same time, there is a time and place to follow the crowd. You do so when it aligns with your preplanned strategy. Then and only then are you allowed to adjust, assuming everything plays out favorably. The most difficult investment decision you will have to make is running against the herd. Conviction is underrated because it's prone to turn into a loss if the decision becomes emotional. This is why **strategic conviction** must be the goal.

What does strategic conviction look like? *"My target sell price is $220, period. This sell price will minimize my loss by 20 percent. I will sell no matter what, I will not try to time the dip. I will not wait for it to drop to $200.* ***This is my strategy and I will stick to it.*** *My other target sell price is $301.30, which will yield a 15 percent upside. I will not sell until the crypto asset reaches one of the sell price targets, period."* This internal dialogue is what strategic conviction sounds like. This is what will save you from the pack**.**

There may be a time where you miss a target sell point and you are thrown into a flurry of emotions. Whatever you do, hindsight will reveal what was right and what was wrong. Return to the qualitative and quantitative drawing board (which we have yet to fully cover) and review the facts. Avoid the herd's influence. Make your decision and stick with it.

POSITION GRATIFICATION

Your final destination for your wealth is what determines what is truly a loss. Is it the overall value of your position in US dollars? Is it

the amount of cryptocurrency you own, separate from fiat? Is it about maintaining a certain percentage of your overall portfolio in crypto?

Traditionally, loss is measured in comparison to a benchmark.[155] If I gain 2 percent on an investment into cryptocurrency, but the S&P 500 gains 7 percent in that same time frame, we consider it a relative loss of 5 percent and then some because of the amount of risk. Retail investors, or the everyday pay people that don't have access to large amounts of capital, typically struggle with this concept, which is why investing in index funds is considered the safest way to earn money.

Let me reiterate that truth here: **index funds are the tried and true way to invest. Everyone should have some percent of their portfolio consisting of index funds.** When you invest in an index fund such as the S&P 500, you are investing in a representation of the US economy.[156] Portfolio composition is talked about in the chapter on principles, and I firmly suggest that a large percentage of your net worth be invested in index funds. A remaining part of your portfolio, which could range anywhere from 0.5–10 percent depending on how much risk you are willing to bear, can be placed in high-risk assets such as cryptocurrency for the opportunity of a higher return.

No discussion on when you lose in investing would be fair or complete without touching on the time value of money and opportunity cost. We will use the common acronym TVM as a replacement for the **time value of money**. The TVM is the concept that money available at the present time is worth more than the identical sum of money in the future because of its potential earning capacity.[157] A dollar invested today is worth more than a dollar tomorrow. Essentially, investing is great, and we should do it now as opposed to later, because money decreases in value when it's not

growing. Not investing money today is technically a "loss" if viewed under this lens.

How about opportunity cost? Hopefully, you have heard of it. Opportunity cost is the loss of potential gain from other alternatives when one alternative is chosen.[158] As it relates to investing, it is the money lost if you would have invested in a different cryptocurrency or asset class. An example would be if your crypto investment went up 10 percent when the majority of other crypto investments went up 30 percent during your investment time frame. You are "losing" money even if on paper you gained. Veteran investors are hyperaware of how their portfolios and investments size up to alternatives and benchmarks.

"I'm always thinking about losing money as opposed to making money. Don't focus on making money, focus on protecting what you have."[159]

—PAUL TUDOR JONES

We must be aware of getting "stuck" in an investment that could have given us better return elsewhere. If your money is not earning money at a solid rate, or if it is not earning at a comparable rate to other common alternatives, then you are "losing" money or failing as an investor depending on how pessimistic you are about yourself. Have an exit strategy for when price drops because of a change in the underlying value of a crypto asset. **It's okay to take a loss.**

"Learn to take losses. The most important thing in making money is not letting your losses get out of hand."[160]

—MARTY SCHWARTZ

You lose money when you sell at a loss. The inverse situation is also true: you can only gain money when you sell. When you actually click the sell button, not before. Lock in your victories or losses, or you

will end up like Simon Golestan, who let his position slowly slip away over time.

Having your Bitcoin be "worth" $2000 more by the market is an increase in your net position only within cryptocurrency terms. Unless you transition back, the "gain" is meaningless. Until the moment you transition back to dollars (assuming this is how you measure your wealth), you have not gained wealth. This is not so with a house, car, or some other asset that has perceived *intrinsic value* by the majority of society—those assets hold their increases in value much better than cryptocurrency. If cryptocurrency were to gain worldwide adoption and reach a critical turning point, then it too would hold onto its value with less volatility overall.[161]

But alas, volatility currently still reigns supreme.

BLACK SWANS

The 2008 financial crisis, the Great Depression, and the COVID-19 temporary stock market dip—these are examples of utterly unexpected financial events that are unpredictable. No one was expecting COVID-19 except a few pandemic professionals. A select set of investors may have been ahead of the curve. But even they were not anticipating the Russia-OPEC oil price war to happen simultaneously. These are all examples of Black Swans: unpredictable events beyond what is normally expected of a situation, typically characterized as "obvious" in hindsight despite being a low-probability event.

A true Black Swan usually results in the price of an impacted asset to be permanently depressed or stuck in a period of negative or low growth for a significant portion of time. Black Swans' precise timing cannot be predicted. If a Black Swan does occur, your reevaluation of what to do with your position (buy, sell, or hold) could be the

difference between losing 20 percent of your money versus 80 percent.

The following is a list of the most likely Black Swan events that would negatively impact crypto:[162]

- Extreme currency devaluation in a major country causing a major market financial crash and subsequently causing the majority of asset classes (including crypto) to crash
- Significant war breaks out on a global scale causing regulations to ban on-ramp fiat exchanges to cryptocurrency for political and economic reasons
- Multiple of the big five banks simultaneously filing for bankruptcy
- Extreme fees for on-ramp fiat movement are announced
- Multiple countries defaulting on debt without major countries supporting a bail out
- A top five largest blockchain protocol is hacked and everyone loses their crypto wealth hosted on that ledger
- A 51 percent attack is consistently carried out against the top five market cap cryptocurrencies (rendering decentralization and security to be broken)
- Market manipulation is discovered among multiple exchanges

These are just a few of the infinite iterations that could possibly cause a domino effect that creates a nearly impossible to predict "Black Swan" event. Many of these have occurred to a smaller degree, but never at the scale described.

I am trying to impart some fear in you right now. If none of those scenarios created even an ounce of fear, you may need to re-examine your basis for risk-reward (you might be a gambler). On a side note, you should also have a plan in case of a countrywide economic crash. It pays in dividends to be prepared for what most people are not even considering as a possibility (those who had extra capital prepared

during the 2008 financial crisis were able to net some amazing returns because they had a plan).

Black Swans have such a distinct impact on cryptocurrency because when major global turbulence hits financial markets, investors move their money from speculative assets into safer assets that they trust, such as index funds or bonds. While the thesis in this book is that Bitcoin and other cryptocurrencies will one day be globally trusted (potentially as a hedge against sovereign currencies), they do not yet operate in this fashion. As such, you must be informed that things can go south. **The thesis could be wrong.** That is the risk you choose to embrace when investing in speculative assets—they are speculative for a reason.

Mastering and successfully navigating the investment world is not just about quantitative models and qualitative investigation. It is also about having profound respect for the ramifications of human behavior.

The truth is that risk is always involved. Principles allow us to manage that risk. Choose to acknowledge risk that could result in loss. Never ignore the possibility of failure. Have strategic conviction and understand the danger of following the crowd. If you embrace these truths, then you don't have to go down with the proverbial Titanic.

---

149 Rob P. Gekwiak,"Lost Money Investing in Cryptocurrency," August 30, 2016, Video, 5:01.

150 Phillip Franklin et al., "The Titanic—Quotes From Survivors," The Titanic, accessed June 2, 2020.

151 Ibid.

152 Ibid.

153 Ibid.

154 Ibid.

155 Christine Benz, "How to Benchmark Your Portfolio," Morningstar, Inc., February 25, 2019.

156 Alicia Adamczyk, "Index Funds Are More Popular than Ever-Here's Why They're a Smart Investment," *CNBC*, September 19, 2019.

157 Edspira, "Time Value of Money (Concept Explained)," September 17th, 2013, Video, 7:00.

158 Marginal Revolution University, "What Is Opportunity Cost?" August 14th, 2018, Video, 2:45.

159 "I'm Always Thinking about Losing Money as Opposed to Making Money.," Valens Research, March 29, 2019.

160 BluFX, "What Is Trading Psychology?," BluFX Blog, accessed June 21, 2020.

161 Luke Fitzpatrick, "The Tipping Point For Mass Blockchain Adoption," Forbes (Forbes Magazine, September 3, 2019).

162 SophonEX, "Does Cryptocurrency Have More Black Swan Events than Other Assets?," *Medium* (SophonEX, March 3, 2019).

CHAPTER 6

INVESTING PSYCHOLOGY—THE RIGHT & WRONG

A young man walks into a casino determined to walk away rich. Walking into a VIP room, he talks to a wide swath of individuals, all of whom had "made it big" in the casino scene. They all point to the slot machines and say this was the best way to become rich. The man approaches the slots with confidence—an old man walks by just as he is about to play. "I'd think twice if I were you before you put everything you own into that machine." The young man laughs and responds mockingly, "Don't you know this is the best way to become rich? I've been informed by everyone in the VIP lounge this is the best kept secret."

The young man put everything he owned into the slot machine.

The young man lost everything.

The young man learned a valuable lesson about survivorship bias.

BEHAVIORAL FINANCE

Investing psychology is an uphill battle. With investing, your mind is at war with some of the most basic human instincts. In an infinitely complex world, decision-makers need cognitive shortcuts. My main goal in this chapter is to tackle the fundamental investing psychology mistakes and make you aware of how easy it is to fall prey to these misjudgments. Hyperawareness of these foundational cognitive issues will make you a much more capable investor.

Meet Shawn Russell, a British property developer. He invested a little under $1,000 in early 2017. As 2017 progressed, he eventually invested $120,000 into cryptocurrency. In November 2017, his net position grew from $120,000 to $500,000. Shawn had little experience with financial products, and he had the perpetual belief the price was going to continue to go up. As the market plummeted in 2017, Shawn lost 96 percent of his overall net worth as he refused to sell while his net position dropped dramatically.[163]

A variety of cognitive factors played into this situation. Why did Shawn not sell earlier when he was up? If you go from $500,000 to $200,000, you are still up $80,000 from your initial $120,000 investment. Why didn't he sell and take a profit while he still had a chance? These the questions haunt so many investors that live through bubbles. Ultimately, this lack of logical decisions ties back to your cognitive biases, greed, and vulnerability to a range of quiet psychological quirks many investors are wholly unaware of.

The purpose of examining behavioral finance is **not** to give you the ability to beat the market. Hersh Shefrin, the author of the first-ever comprehensive piece of literature on behavioral finance, stated, "I think most investors are overconfident about their vulnerability to psychologically induced errors, and although intelligent, [they are] not as intelligent as they believe themselves to be."[164] The purpose of an investigation into behavioral finance is to help you avoid financial mistakes by spotting and avoiding dangerous cognitive shortcuts and biases attached to your investing tendencies.

BIASES & SHORTCUTS

Cognitive biases are the ways we diverge from rationality within our judgement. To be irrational is, at the core, to believe in something that is not reasonable or logical. We have many cognitive

weaknesses as well; certain scenarios (high risk and high pressure) are more likely to draw out irrationality. Recognizing which cognitive biases are consistently threatening us, as well as what scenarios bring out these biases, results in safer investing.

- Evaluation Bias of Conjunctive and Disjunctive Events[165]

People tend to overestimate the probability of conjunctive events (e.g., all fifteen steps of my home-improvement project will happen without any hiccups). The more events that need to occur before a certain outcome, the less likely it is to occur. For example, in order for x price to occur, developers need to do A, B, C, D, and F. The more events needed for a fundamental price change to occur, the less likely it is to happen. And yet while this is intuitive, research has shown people don't account for additional conjunctive events' impact on the likelihood of the outcome.

The inverse of this rule is also true; people tend to underestimate the probability of disjunctive events (at least one part of my thesis will go horribly wrong, leading to a terrible sequence of all-nighters). Essentially, our brains often ignore worst-case scenarios. As a teenager, you might have heard of the Superman complex. Evaluation bias of disjunctive and conjunctive events is the adult version.

An illustration of this bias can be seen in the exuberance during a bull run. Oblivious investors ignore the possibility of bad news. Discounting the possibility of anything going wrong tends to result in investors being "surprised" when a negative piece of press makes its way online—resulting in a volatile price swing that hurts their overall position. Another case is an investor sinking cash in a new cryptocurrency based on the road map of development laid out by the developers. The investor's conjunctive bias assumes everything

will occur in succession with minimal hiccups, much to their chagrin when significant friction is encountered.

•Biases of Imaginability[166]

Your memory is biased. You might not like it, and I don't blame you. At the end of the day, your memory damages your investing judgement. Here is how: you under-rehearse unpleasant memories, leading to biased, availability-based inferences.

The inverse is also true. We over-rehearse pleasant memories.

This bias is represented by many investors during a long-drawn-out bear market—investors will make decisions as if at any moment there will be a replica of the last bull run. Another illustration takes place during a bull market after a long-drawn-out bear market. Because the investor has been "stung" so many times by the investment, when the price finally starts to trend upward, the investor is controlled by the euphoria of the price movement. This under-rehearsal of an unpleasant bear market corners the investor into throwing away the fundamentals as they simply choose to dangerously ride the price upward as an emotional decision as opposed to a logical one.

•Biases of Availability

People assess the frequency of a situation or the probability of an event by the ease with which instances or occurrences can be brought to mind.[167] This is why being an experienced investor allows you to be more in tune with the ebbs and flows of the market. A drastic drop or pump in price for someone who has seen it happen hundreds of times is more likely to react in an unemotional strategic way compared to someone who has not been in the same situation as frequently. Journaling also helps reduce the impact of this bias.

- Insensitivity with regards to regression towards the mean

Extreme outliers tend to regress toward the mean in subsequent trials, and intuitively, we expect subsequent trials to be representative of the previous trial.[168] As a result of this insensitivity, people fail to anticipate regression to the mean. This is apparent in how people expect the market to behave after/during an extreme bull or bear trend. Our minds don't want to accept the highly probable event that the run was an outlier. You will see people claiming that the fundamental underlying value of said asset (during the run) has changed, when in truth the trend was a statistical outlier that has a high probability of returning to the mean at some point in the future.

- Insensitivity to Predictability

Predictions are often made by representativeness.[169] In other words, if a cryptocurrency is described favorably (lots of incoming updates/upgrades) we predict outcomes that are similar (new investors and a higher price). What is not taken into account is the reliability of the information. This is a sobering insensitivity. We trust too quickly and expect too much. Unfortunately, your job as an investor is to make decisions based on information that is oftentimes incomplete. The best thing you can do is strive to obtain quality information to help battle the difficulty of making predictions with imperfect information.

- Insensitivity to Sample Size

Insensitivity to sample size in investing is a cognitive bias that occurs when people judge the probability of predicting an outcome without respect to the sample size.[170] Variation is more likely in smaller time frames, but new investors are not necessarily cognizant of this. As a result, those with less time in the market have a smaller

sample size and are often unaware of the bias they have toward short-term trends when first jumping into the investing game. This is detrimental to quality decision-making. Insensitivity to sample size is why new investors tend to act overconfident about their decisions.

MY DATA INSENSITIVITY

In early 2018, this cognitive bias had a deep impact on me. As a first-time investor, I was checking the charts every couple of minutes. I would pull up my phone and watch the market move on a one-minute time scale. Because I had such little time in the market, I would go from having conviction everything was about to soar to, only a couple of hours later, believing the price was going to collapse permanently.

Glued to the chart, I was hyper-focused on every little trend change. My sample size was terribly small, and I had almost no long-term strategy to speak of. After many quick trades, I quickly realized I needed to learn to observe and invest in long-term trends using larger sample sizes other than just a week's worth of data. While I feel somewhat embarrassed to reflect on what I looked like as an investor at the beginning, in hindsight it is apparent many biases were battling (and winning out) over me!

- Survivorship Bias

Dead men don't tell tales. Neither do investors who lost big. People flock to successful investors, not accounting for the fact that their track record may be very short. In addition, people generally feel that everyone around them is making it big with investing. This is mainly because the majority of voices are those who are successful or claim to be successful. Be aware of this dynamic! Whether

someone is selling you investment services or advice, think about the survivorship bias and how you might be jumping to an inaccurate conclusion as a result of an incomplete picture.[171]

JOURNALING

Our brain fundamentally does not process with a consistent, logical approach. Be wary of your memories. **This is why journaling your investment thoughts and decisions is so important.** Journaling allows you to overcome memory discrepancies by giving you a snapshot of your mindset during all the turbulence of investing.

Christian Ryther, founder of Curreen Capital, is a strong believer in investment journals. He commented in early 2019, *"I think investment journals are underestimated as a tool—a big part of the benefit comes from reducing errors and mistakes. As humans we don't like to think about mistakes because it doesn't fit the narrative our ego creates that tells us we are consistent and correct in our thoughts."*[172] What does an investment journal look like?

An investment journal consists of the following entries:

- The date
- The asset
- Why you are invested
- How much you own
- Target sell price
- Target buy price
- News and developments

By updating this type of journal every seven days, you give yourself the opportunity to be able to view your emotional and cognitive fluctuations over the course of time relative to price movement, news, and fundamental changes. This type of journal is invaluable as

you begin to understand your investing instincts. As Christian Ryther states, *"Your job as an investor is to have an accurate view of reality and an accurate view of yourself to better understand how to make investment decisions with incomplete information. Investment journals give you clarity about a variety of risks, and answers questions that arise."*[173] Learn to view yourself with a historical lens and you give yourself the chance to not fall prey to making uninformed, spur-of-the-moment investment decisions.

COGNITIVE WOLVES

Let us now move on to the broader pastures of cognitive biases. The following make up the seven deadly cognitive wolves that are lethal to everyday investing sheep:

- Fear of Regret
- Overconfidence
- Anchoring
- Hedonic Editing
- House Money Effect
- Loss Aversion
- Winner-Loser Effect

Fear of Regret is the enemy of the everyday investor. It's that moment when you check the charts to see how your investments are doing, read an article about an investment you don't know, and as a result feel that "itch" to sell your current investment while simultaneously jumping ship to a new one. The problem with FOMO (Fear of Missing Out) is sometimes it **does** work. More likely than not, though, it is for all the wrong reasons. Decisions based on a feeling of fear and greed will slap you down more times than they will help.

A proverb I believe captures this fallacy is ***"Hasty climbers have sudden falls."*** Making a series of hasty, fear-based decisions might work once, twice, or maybe even three times in a row. But all it takes is one of these emotional decisions to throw you off the proverbial cliff.

A huge chunk of your investment portfolio could disappear with one hasty decision, leading to a series of more fear-based investments to make up for the loss. I know countless stories of traders chasing gains after losses. But the truth is that you can drive forty miles to the nearest casino and the Fear of Regret is clearly evident. This is not solely an investment phenomenon. It dictates how we view gains in relation to risk. FOMO can only be mitigated with discipline and a plan.[174]

As Publilius Syrus, a famous Latin writer from 85 BC, put it, *"Anyone can hold the helm when the sea is calm."* Patience, strength, and discipline are the characteristics you must build up in order to be resolved enough to not act on FOMO when it attempts to throw you overboard.

For those invested in an asset that rapidly gains value, FOMO is easy to avoid because you are already riding a wave of success. And yet, as a bubble continues to develop for those riding the crest, FOMO begins to damage an investor with an amazing net positive position.

I have seen investors convinced an asset is going to go from $900 to $20,000 after the asset already saw an absurd 200 percent growth from $300 to $900 in a matter of months! These are the individuals that have made a once-in-a-lifetime investment, and yet the cognitive bias of FOMO still prowls around on these successful investors. FOMO preys on the greed and fear that believes the

growth of an asset will continue, even if this type of asset price growth is logically unsustainable.

Overconfidence is a closely related cousin to FOMO. People tend to set overly narrow ranges of possibilities for price on medium time ranges, not accounting for huge swings downward or upward as a result of unforeseen events and market conditions.[175] In other words, every investor has some small percentage of their mind that believes the lie that they can predict the future and the range the price will fall within.

In addition, people tend to believe the price of an asset can only drop so low when it starts to enter into its own bear market, often causing people to try to catch the "falling knife." While people scoff at the idea of being someone who would try to grab on and play such a dangerous game, because people set overly narrow price ranges subconsciously, when the price falls past their subconsciously narrow price range, they will often say to themselves, "This is a steal of a deal. Surely it will not go lower. The bottom is in." The market wolves love to pick off and devour overconfident investors. When you are working with your financial well-being and safety, there is no room for ego in decision-making.

This idea of narrow confidence bands and price prediction all tie back to anchoring. **Anchoring** is a psychological effect that causes people to consciously pick a price for what an asset will be one day valued as. This is not bad; models exist to do this for us. Here is the problem: **anchoring, as a bias, chooses to ignore the effect of new information on the target price.**[176] This is illogical, but a consistent phenomenon across every level of financial prediction. How can anchoring be avoided?

You must be ready to readjust your predictions based on new fundamental improvements to a crypto asset or underlying blockchain protocol. This is why journaling is so imperative. If you find yourself having a static number that you are waiting for an asset to reach, and news comes out but you do not change this price point, stop yourself. Update your investment journal by accounting for the new information.

As a wise colleague of one of my university projects said, "Blessed are the flexible, for they will not be bent out of shape." If you refuse to "flex" your target buy or sell price because of new information, then you are falling prey to price anchoring.

Hedonic Editing is a strange effect that stands alone in this pack of wolves. Hedonic Editing is the effect in which the frame and model with which you view a certain investing situation, and even the language involved, fundamentally alter the way you view a gain or a loss.[177] An example of this is when professional investing consultants and asset managers use language concerning net positions. When talking about "closing an account," people get extremely uncomfortable and unhappy with their investment decision. When the language is altered to "transferring an asset," suddenly people are much more open and excited about what is to come, even if both sets of language describe a loss.

This effect comes into play with dividend-based stocks versus non-dividend-based stocks. A stock that is operating at a loss from the initial purchase price point without dividends will cause investors to feel a strong sense of loss. Add in a dividend, and suddenly the entire frame of mind people operate with is altered: "It's okay, I am getting steady dividends from this, it will pay off in the long run."

I suspect this exact effect will come into play once staking and dividends with cryptocurrency are fully implemented into blockchain protocols such as Ethereum. As of right now, the potential to be able to receive some sort of valuable dividend from owning a certain amount of a crypto asset is highly sought after and speculated over, far past the point of reason. The effect language has on our frame of mind cannot be underestimated. Where you get your information from is imperative to forming the lens with which you view the investing world. You must be careful with how you allocate weight and authority to the resources you read and consume relative to your crypto investments because of the danger of Hedonic Editing skewing your view of reality because of the language used.

One of my favorite effects to talk about is the **House Money Effect** because it has plagued my mindset as an investor ever since my first investment.[178] It goes as follows: people who are "in the green" are more likely to take risks at a disproportionate rate than if they are not in the green. Say I give you a twenty-dollar bill. You are more likely to be willing to take a risk with that twenty dollars than if you started at zero dollars and had to pull out your own twenty-dollar bill. If your twenty dollars turns into forty, you are more likely to take a risk with that forty than if you had to start from scratch with a new twenty-dollar bill. This is perfectly illogical, and once again not surprising.

How much better would your investment decisions look if you never knew whether you were operating at a loss or a gain? If you were operating under the assumption you are breaking perfectly even, your decisions would look a whole lot more levelheaded and logical, as you wouldn't know you were returning +56 percent or –32 percent on investment. The House Money Effect is merely a reflection of human greed and the ability to pull off mental

gymnastics as justification for making continuous high-risk decisions in order to validate FOMO.

Loss aversion is typically the term the financial world gives to individuals who are low risk.[179] While this is true, I would also like to observe that individuals influenced by the House Money Effect (when in the red) will often take extreme gambles with their investments in an attempt to recoup a loss. This is because "gambler" personality investors are often incorrectly quantified relative to risk aversion. They are not "risk" averse in the traditional sense—they are loss averse.

These loss averse investors are comfortable with high levels of volatility with their decision-making in order to no longer be at a loss. Thus, these individuals are "risk averse" in the sense that being in the red is a "risk." Their sense of risk is oriented based on their net position and are so risk averse that they take highly volatile positions to escape a loss. Despite being contradictory from a definition perspective, from a behavioral finance angle this type of investor logic unfortunately checks out and is all too common in cryptocurrency markets (or casinos) where volatility abounds.

If you are a high-risk individual, understanding your loss aversion profile is paramount to becoming a safe and consistent investor. Financial discipline means being able to walk away from the charts if you have the "sudden inspiration" to immediately make a purchasing or selling decision. If your gut instinct is telling you to make a decision right this moment, this should give you immediate pause.

If the impulse decision is truly a solid fundamental long-term play, then waiting twenty-four hours will not drastically change the playing field. What twenty-four hours does is give you the

opportunity to objectively pause and evaluate the following set of questions: Have the fundamentals of the asset changed? Has the narrative changed? What does the most recent investment journal entry target and why?

If you are a high-risk individual reading this book, the one thing I would have you walk away with is, before you make any split-second decision, pause and force yourself to walk away and come back in twenty-four hours. No, not fifteen minutes or thirty minutes. Twenty-four full hours.

Dr. John Grohol, CEO and founder of Psyche Central, suggests that unconscious thought, contrary to the way many of us think about it, is an active, goal-directed thought process.[180] The primary difference is that in unconscious thought, the usual biases that are a part of our conscious thinking are absent. In unconscious thought, we weigh the importance of the components that make up our decision with greater equity, leaving our preconceptions at the door of unconsciousness. **If you detach yourself from the situation with a full night of rest, you will realize the vast majority of decisions are tainted by your emotions or by one of the cognitive biases explored in this chapter.** Stick with your principles and your long-term price targets for your buying and selling decisions. Don't trust sudden inspirations.

The corollary to sudden inspirations is individuals who make no decisions at all. Loss averse individuals psychologically abhor selling at a loss so much that they hold onto losses for far too long. Shawn Russell was a prime example of this. Instead of cutting losses on the way down, Shawn was so loss averse he couldn't stand to cut his losses. Anecdotally, loss averse investors, especially those with minimal investing experience, typically don't have long-term price targets.

Shawn Russell is a perfect example why having a preplanned price strategy (using our investment journal) is imperative. What does this look like in action? Simple. “If this asset falls to x price as per my investment journal valuation, I am selling no matter what.” I have found that individuals without exit plans tend to be loss averse individuals who believe they can just ride out the market. They use an extremely long time horizon as an excuse for bad decision-making.

Unfortunately, the time value of money comes in to play here. Experienced investors will tell you to follow an exit strategy and reallocate your wealth to a different asset that will grow your overall net worth. Time and money invested in a slowly sinking asset are way more expensive than is immediately evident because of the opportunity cost that grows from the time value of money. Don’t sit with losers for too long. Selling at a loss is okay. It will happen, and you will be much better off in the long run by being willing to exit at a loss as opposed to refusing to ever exit at all. In addition, exiting at a loss will allow you to potentially repurchase the asset at a lower price, growing your overall position. Loss is not a permanent scar on your overall portfolio—you can recover if you give yourself the chance.

Transitioning to the **Winner-Loser Effect,** we find a close sibling of loss aversion. The Winner-Loser Effect is the phenomenon of security analysts, financial “experts”, pundits, and individual investors showing a bias toward recent successes in their predictions and investments. This makes “logical” sense in that something we believe is having a series of successes will naturally continue to have success. While generally this statement could be seen as true, it is the rate of predicted successive successes that gets twisted. The

inverse is also true: the rate of predicted successive failures for losing investments tends to be drastically overestimated.

In 1997, the International Monetary Fund released "Winner-Loser Reversals in National Stock Markets: Can They Be Explained?" evaluating the Winner-Loser Effect on national stock market indices over the course of the previous decades.[181] DeBondt and Thaler in 1985 were the first to identify the Winner-Loser Effect. Since then, a variety of other research has proven the legitimacy of this trend that good assets/indices will continue to do well, and bad assets will continue to do bad over the course of ten to twenty years. The problem, then, is, When does this ten to twenty-year period begin? Investors who fall prey to being biased by the Winner-Loser Effect will only be right (or wrong) in hindsight.

A variety of "technical analysis" experts will encourage the viability of "momentum" over long-term time frames based on these studies, but giving too much decision-making clout based around this idea is dangerous. The crypto sphere has an obsession about blockchain protocols releasing news. Investors drool over announcements, marketing campaigns, and public media because they feed right into the Winner-Loser Effect cognitive bias for both winners and losers. This is why you must track deadlines of project timelines and adjust your pricing expectations and predictions based on the actual fundamental progression of a blockchain project.

This chapter's topic could easily be its own separate book. A vast wealth of information is out there that I would encourage you to pursue. *Beyond Greed and Fear* is a book I believe every investor must read before they spend a single penny in any volatile market.[182] I wish I would have read it before I started on my path as an investor because it showed me just how complex and irrational every single human being is. Add financial stakes and complex markets with high

amounts of volatility (e.g., crypto assets), and you are left with an environment ripe for emotional decision-making.

Reader, the better you know yourself and your tendencies, the more likely you will be able to spot impulse decisions and stop yourself in your tracks. Learn to recognize and discern your best and worst qualities as an investor and I promise you will be financially, psychologically, and emotionally better off. Yet investing effectively is more than just being able to identify the best and worst in yourself.

Ultimately, in the blockchain investment sphere is an arms race among informed and misinformed individual investors (all impacted by cognitive biases to varying degrees) who are desperately trying to recognize undervalued and overvalued blockchain projects. The next chapters will take the deep dive into walking you through the set of variables, factors, people, metrics, and qualitative information that will help you accurately inform your investment decisions.

---

163 Michael Kaplan, "Bitcoin Crash: This Man Lost His Savings When Cryptocurrencies Plunged," CNNMoney (Cable News Network, September 11, 2018).

164 Hersh Shefrin, "*Beyond Greed and Fear: Understanding Behavioral Finance and the Psychology of Investing,"* (Oxford: Oxford University Press, 2007).

165 Royce IP, "The Conjunctive and Disjunctive Events Bias," Farnam Street, January 18, 2016.

166 Daniel Kahneman, *Thinking, Fast and Slow,* (Random House, 2011).

167 lbid.

168 Bhala, Kara Tan, Warren Yeh, and Raj Bhala, *International Investment Management: Theory, Ethics and Practice*. London: Routledge, Taylor & Francis Group, 2016.

169 Mohammed Alkhars et al., "Cognitive Biases Resulting from the Representativeness Heuristic in Operations Management: an Experimental Investigation," *Psychology Research and Behavior Management* Volume 12, April 10, 2019.

170 "Sample Size Fallacy," Oxford Reference, accessed June 3, 2020.

171 Edwin J. Elton, Martin J. Gruber, and Christopher R. Blake, "Survivor Bias and Mutual Fund Performance," *Review of Financial Studies* 9, no. 4, 1996.

172 Cureen Capital, "Investment Journals: Not for the Weak," June 4, 2019, Video, 13:12.

173 lbid.

174 John M. Grohol, "FOMO Addiction: The Fear of Missing Out," World of Psychology, July 8, 2018.

175 Sweeny Kumar, "Behavioural Biases and Their Effects on Investment Decisions Series—Part 3," ValueWalk, February 1, 2020.

176 Sweeny Kumar, "Anchoring Bias And Their Effects On Investment Decisions Series—Part 10," ValueWalk, February 1, 2020.

177 Vakkur, "Behavioral Finance—Evidence For Heuristics," *Behavioral finance*, Accessed June 3, 2020.

178 Corey Hoffstein, "Investors Beware The House Money Effect," *Forbes* (Forbes Magazine, January 21, 2016).

179 David Gal, "What Does Loss Aversion Mean for Investors?," *Psychology Today* (Sussex Publishers, May 16, 2019).

180 John M. Grohol, "Why 'Sleeping on It' Helps," LiveScience (Purch, October 26, 2009).

181 Anthony J. Richards, "Winner-Loser Reversals in National Stock Market Indices: Can They Be Explained?" *IMF Working Papers* 97, no. 182, December 1997.

182 Hersh Shefrin, "*Beyond Greed and Fear: Understanding Behavioral Finance and the Psychology of Investing,"* (Oxford: Oxford University Press, 2007).

CHAPTER 7

ON WORDS FROM THE WISE

A fool repeats history. A greater fool ignores the advice of those who have lived through history. In this chapter, we will examine some of the wisest investing quotes, ideas, and misunderstandings that have stood the test of time. Destroy the idea that people make it big by luck; it is a fruitless deception that is completely counterproductive to the psyche. Investing wisdom combined with hard work is what will lead to success over the long haul.

Let us begin with advice from our good friend Benjamin Franklin: *"An investment in knowledge pays the best interest."*[183]

I start with this because I once had a friend approach me concerning cryptocurrency investing. I had been talking to him about blockchain technology for about sixty seconds. He stopped me and said, *"Carter, I'll just give you my money and you can invest it for me. I trust you."*

In that moment, I looked him in the eyes and laughed.

It was an intense fit of laughter followed by a long silence. He looked confused and said, *"I don't understand, why are you laughing?"* I told him the truth. *"Never trust someone else with your money, and on top of that, never invest in something you can't explain."*

When we take Benjamin Franklin's advice and invest into our own knowledge of blockchain, we are rewarded with being able to understand what truly valuable projects look like.

The knowledge that is gathered by deeply investigating and researching the various white papers, programmers, GitHub repositories, researchers, network statistics, news, and development road maps is what amounts to foundational knowledge that gives us real direction in our investment decision-making.

Too many people expect information that is truly valuable to be handed to them on a platter. If you want crypto investing success and if you want the type of knowledge that "pays the best interest," you must go out there and dig for it. You have to grind through the piles of mud to find the pot of gold. There are no 100 percent promises in crypto. No one ever promised you universal success with every single one of your investments.

In summary of Benjamin Franklin's quote, when it comes to investing, nothing will pay off more than educating yourself. Do the necessary research and analysis before making any investment decisions. Strive to have unemotional and objective investment conviction. Only then are you truly leveraging the power of the information itself.

THE ORACLE OF OMAHA

Warren Buffett is a name whispered in awe by both amateur and professional investors. One does not talk about investment advice without recognizing Buffett as a prime vault of wisdom; precious advice from this vault of knowledge has been given out to us all for free. Ironically, it seems Buffett is not the biggest fan of the crypto space! Nevertheless, we will extract the wisdom he has had from his direct experiences and apply his wisdom to our own situations and investments.

Investment risk is defined as the probability or likelihood of the occurrence of losses relative to the expected return on any particular

investment.[184] Stated simply, it is a measure of the level of uncertainty of achieving the return as per the expectations of the investor. Investors in the upper echelon believe lack of knowledge increases your total risk. As Warren Buffett pointedly puts it, *"Risk comes from not knowing what you are doing."* While this may be a slight exaggeration as there is always "risk" in any market, his thoughts seem to line up with Benjamin Franklin's. Reduce your level of uncertainty by exploring the factors that would make your investment decision uncertain.

This might sound like a simple idea, but so many people jump into borderline gambling because of a lack of awareness surrounding investment risk. These optimistic and often new investors will convince themselves opening leveraged longs or shorts on a cryptocurrency is a brilliant idea. Worse, some commit all their capital to just cryptocurrency without any diversification into other asset classes such as precious metals, stock, bonds, real estate, etc. This can result in a rather costly and disheartening first encounter with crypto.

Frustrating and disastrous failures can be avoided by tempering emotional investing with solid fundamental analysis of why you are about to make your move on an investment. Following a method for investing using a quantitative model, which generates a price target, parallel to your qualitative investigation helps reduce overall investment risk.

To quote Peter Lynch, *"Know what you own, and know why you own it."* Knowing why you own something cannot be repeated enough. Do your homework before deciding. And once you've decided, make sure to reevaluate your portfolio on a timely basis using new information —if you don't, you are at risk of anchoring bias. A wise holding today may not be a wise holding in the future.

Here is a shortcut to knowing if what you are about to purchase/invest in is a good idea, according to Warren Buffett: *"Only buy something that you'd be perfectly happy to hold if the market shut down for ten years."* Reread that—seriously. This is the apex of what fundamental investing circulates around. Write it down. Memorize it. Let it be your creed. This is the type of mindset you must adopt to set yourself above the pack. Pick the winners that will be around in the next five to ten years, not the ones that will skyrocket for only a day or two, and then fade into oblivion.

PARABOLIC STUPIDITY

Parabolic growth. Soaring prices. Numbers in the green. Consecutive days of massive growth. Endorphins. Elation. Greed.

"Every once in a while, the market does something so stupid it takes your breath away."

—JIM CRAMER

Parabolic growth is an uptrend in price in which the angle of ascent increases as time continues onward in the shape of a parabolic function. Parabolic growth is fueled by retail money and FOMO. Parabolic growth cannot be maintained because of the laws of economics. The opportunity cost of alternative purchasable items will eventually come into play, as well as the fact that our planet has a finite amount of resources.

Suri Duddella, an analyst who specializes in the impact of sentiment swings on price, found that **post-parabolic growth typically sees a 62–80 percent reversal in price on average**.[185] Gold prices from 2000 to 2011 are an excellent example of this: prices increased from a mere $200 all the way to $1,800. Naturally, 2013 saw a drastic

downswing back to $1,100. The NASDAQ's parabolic growth from 1995 to 2000 saw an 80 percent retracement in price![186] Talk about volatility.

"But a pin lies in wait for every bubble. And when the two eventually meet, a new wave of investors learns some very old lessons: First, many in Wall Street—a community in which quality control is not prized—will sell investors anything they will buy. Second, speculation is most dangerous when it looks easiest."

—WARREN BUFFET

Be wary of parabolic growth. If you see an asset double in value in under a month, you should look for an exit point. **Don't get greedy.** If you are in the green, look to exit once a reversal is in sight.

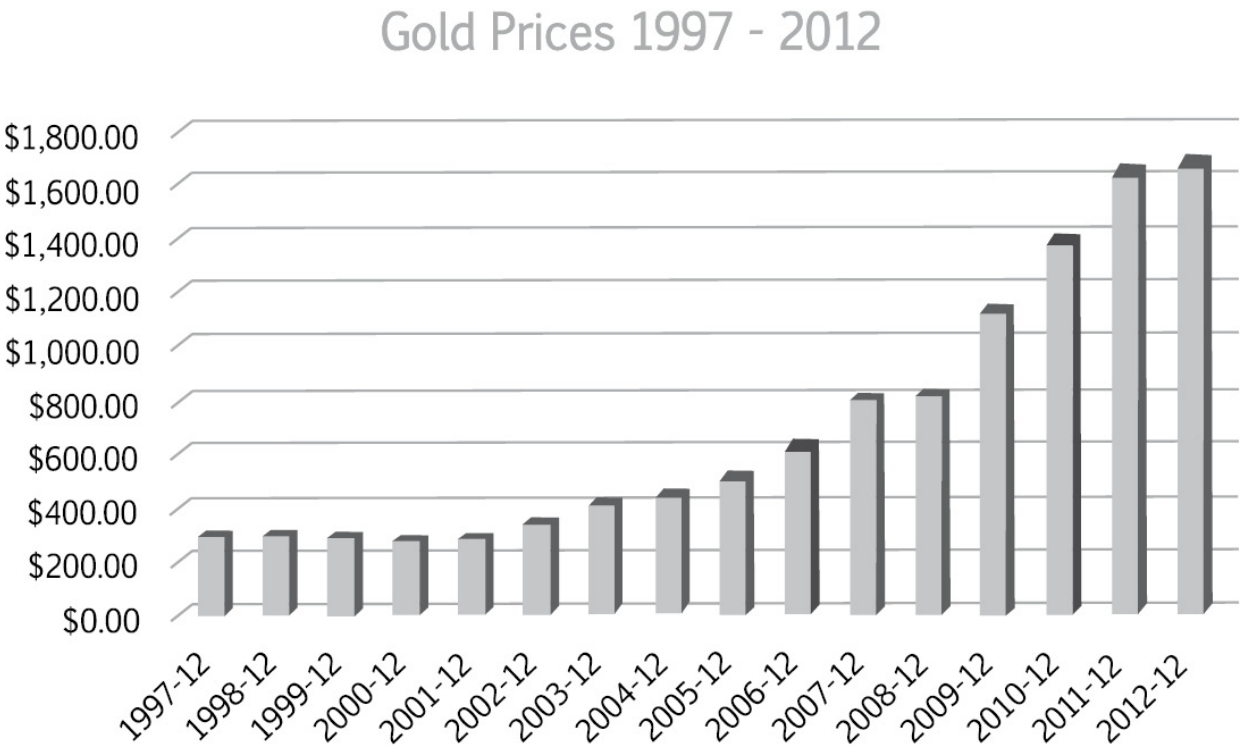


Figure 8: Gold Bubble

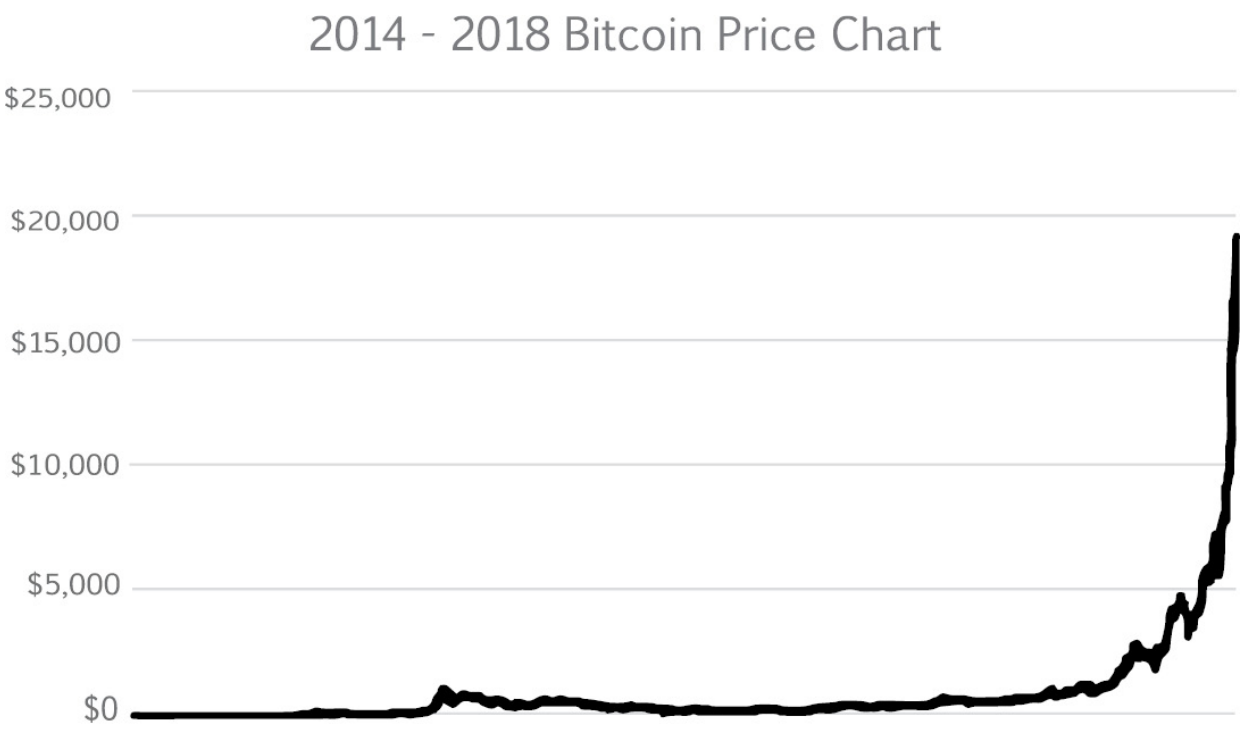


Figure 9: Bitcoin Bubble

This chart was the price of Bitcoin from 2014 to 2018. During a five-month time frame, Bitcoin saw a nearly 250 percent increase in price. Naturally, this wasn't sustainable. Any investor who saw a 2x in money ($100 becomes $200) should have been looking to exit. These types of gains are unheard of. They don't last. A vapor in the morning. Collect it while you can, because it will dry up quickly in the heat of the market.

Many people refused to sell during and after the drastic price increase. Fortunately, most of these investors will be fine in the long run because cryptocurrency continues to grow as an asset class. Despite this, these investors could have grown their wealth if they had chosen to be less greedy. Instead, they did not increase their net worth because they were stuck waiting for the price to return or exceed where it once was before.

This is unfortunate, but altogether preventable, if a principled investment plan were in place. Beware of bubbles. If you are on the

profiting end, financial bubbles are some of the most amazing opportunities. You are better off incrementally locking in gains than losing all of your potential gains to a lack of planning and greed by refusing to sell even a portion of your cryptocurrency.

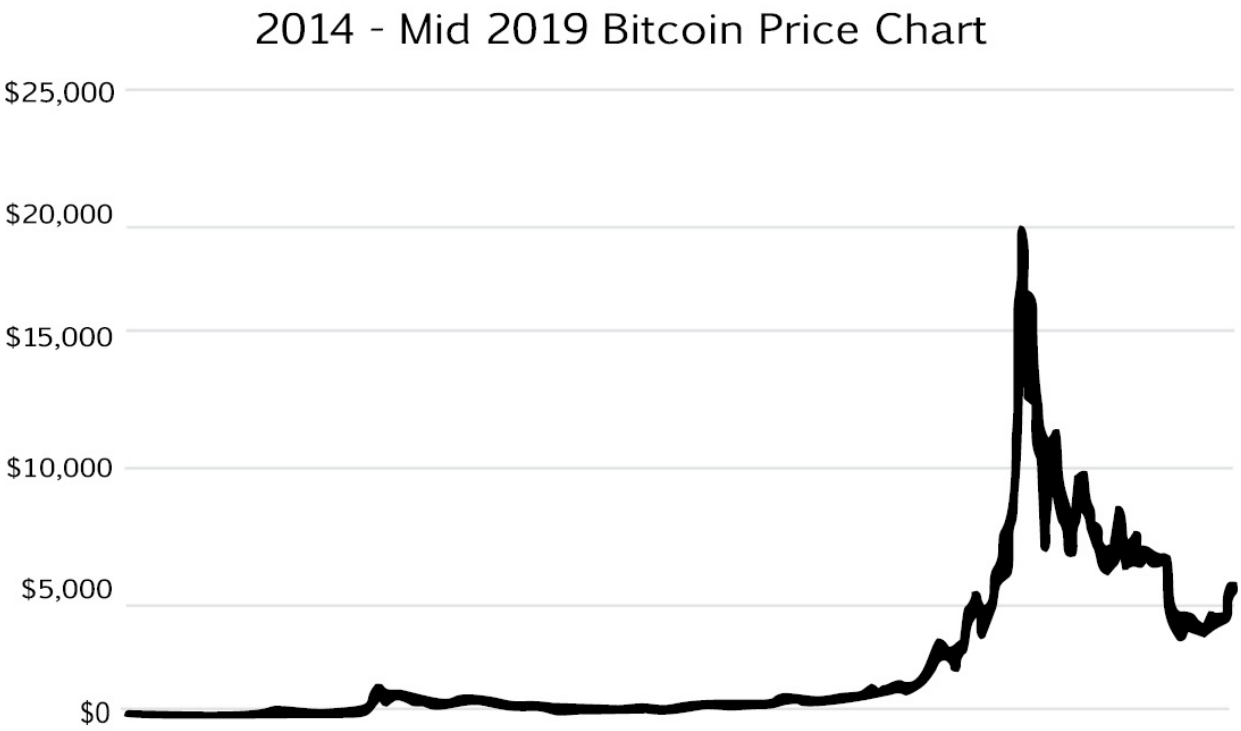


Figure 10: Bitcoin Bubble Boom & Bust

TO SPOT A BUBBLE

As Warren Buffett puts it: *"It's only when the tide goes out that you learn who has been swimming naked."* To put it bluntly, only after a bubble corrects can we see who had investing principles and who did not. Part of what acting on investing principles means is having a target sell price, a reason for the sell price, and the courage to carry through in the face of behavioral factors fighting against that instinct —to be resolved in the face of greed or fear.

A common occurrence in asset classes that have seen such absurd volatility (such as cryptocurrency) is to hear people say, *"There will*

never be a bubble again." This is typically touted by new investors who got burned by a bubble and understand at some point in time they had a huge opportunity to grow their wealth. Post-bubble, as time progresses and the market stabilizes, people fall into the cognitive trap of believing two ideas. First, people assume if a bubble occurs again, they will act rationally and thus don't need a plan. Second, they believe other investors will act rationally in the face of a bubble occurring again.

Both ideas are false.

> *"What we learn from history is that people don't learn from history."*
>
> —WARREN BUFFET

But what precisely characterizes a financial bubble? What types of buzzwords can we look for in our crowd mentality that signal we should step to the side before following the cattle off the cliff? While any variable listed below in isolation is no guarantee of a bubble, a combination of a couple of these should set off alarm bells in your investment journal and investigative work.[187], [188]

- Extreme media attention on an asset that traditionally does not receive attention
- Investors rationalizing lending, borrowing, and purchasing based on the expectation of the price increasing (as opposed to the fundamentals that make the asset intrinsically valuable)
- Factual evidence of a drastic increase in investors purchasing on margin
- Rationalizing price by weak arguments, such as "this time it's different" or "prices only go up."

- Hostility toward individuals who are skeptical about the drastic price increase
- Distinct lack of quantitative and qualitative model discussion
- Investors actively trying to convince others to purchase the assets
- Volatile change in ratios that have had historical significance (such as 2–3x price increases past all-time high price)

You have an opportunity to be outside of the crowd: an anomaly in the face of greed, ignorance, and downright stupidity. Master this list, and the world will open up to you. Even if you can't spot bubbles, and the model and variables presented here are flawed, you still give yourself an advantage.

"In the land of the blind, the one-eyed man is King."[189]

—DESIDERIUS ERASMUS

Later chapters will give you additional skills to navigate and have a plan inside and outside of bubbles. For now, rest easy in the knowledge that the first step to profiting or avoiding a bubble is to first be aware of their existence.

SUCCESS

"If you look really closely, most overnight successes took a long time."

—STEVE JOBS

This is true of investors and investments. Much of the advice that exists in investing orbits around the idea of taking risks while also having patience. Because of inexperience, new investors feel the impulse to make decisions. They want to play the bubble to its fullest.

They dive in, touting the fact that the only way to be successful is to take risks.

The bottom of the proverbial pool hurts—and it's almost always a surprise when an investor bumps into it. Impulse decisions are not sustainable.

I would make an addendum to this simple truth. The best investments you will ever make are founded in taking a long-term risk on a long-term growth proposition. This is because just as the best companies and blockchain protocols are not built overnight, neither is the case for your investments. Treat risk as the greatest mentor, one that will punish you for being brazen and reward you for wisdom.

"There is a difference between the irresistible impulse, and the impulse not resisted. And that is why the best thieves don't get caught."[190]

—EFRAT CYBULKIEWICZ

Maybe you will get lucky. Maybe you will invest in a "moonshot" coin. Maybe. But don't count on it. The cryptocurrency casino is open twenty-four seven, 365 days a year globally. Know your investing fundamentals and understand the wisdom of those who have gone before you or suffer the consequences.

I've ranted and raved about fundamentals and taking responsibility. This is done by having investing principles. But what exactly are principles in crypto investing and how do we apply them to our investing strategies?

---

183 Benjamin Franklin et al., *The Way to Wealth: Preface to Poor Richard Improved, 1758* (New York, 1953).

184 James Chen, "Risk," *Investopedia*, March 27, 2020.

185 Stocktwits, “The Parabolic Arc Pattern or How To Profit from Euphoria and Bubbles,” Medium, (The Stocktwits Blog, May 18, 2017).

186 Ibid.

187 Scott Galloway, “An Economic Bubble Is about to Burst, and These Are the Very Clear Warning Signs,” *Business Insider*, May 30, 2019.

188 “Top Anecdotal Signs of a Market Bubble,” bmcamcom, September 9, 2017.

189 Desiderius Erasmus, *Adagia* (Basileae: In aedibus Ioannis Frobenii, mense Octobri, 1520).

190 Efrat, “Efrat Cybulkiewicz,” America-Israel Cultural Foundation, April 26, 2019.

CHAPTER 8

PRINCIPLES

A stockbroker was hospitalized with a fever. When a nurse walked into the room and took his temperature, the stockbroker asked, "How much is it?"

"102, sir." the nurse replied.

The stockbroker furrowed his eyebrows with intense focus.

After a moment of contemplation, he settled on a plan. "Sell it when it gets to 103."

Stick with principles, not your gut. If our gut instinct was typically correct, we would all be millionaires. Returning to our investing creed (courtesy of Warren Buffett), *"Only buy something that you'd be perfectly happy to hold if the market shut down for ten years."* Markets will always be full of chaos. This is why principles are so critical. **Principles are what you can control.** The following are the key principles investors control:[191]

- Goals
- Balance
- Cost
- Discipline

Warren Buffett's first televised interview back in 1985 speaks to these. *"A short-term focus is not conducive to long-term profits."*[192] Having lived through the cryptocurrency bubble of 2018, investing principles were lacking. The hype of where the price would be

tomorrow seemed to loudly overpower any discussion about justification for where the price could be in five years. If I could rewind the clock, I would have sat myself and other investors down and asked some simple questions.

"What are your goals? Is your portfolio reasonably balanced between multiple different asset classes? Do you have a target exit price? Do you have the discipline to stick with your plan?"

I imagine an investor without principles feels on edge and wired up constantly. They are running at full speed, dodging any semblance of an obstacle that would "slow them down"—a type of madness intertwined with greed that refuses to confront the simple questions.

The hard truths—**Investing principles are the truths your capital lives by**. Respect what it means to establish principles. Give yourself the chance to slow down and establish your investing principles before a market turns chaotic, so when everything is in motion, you are standing still knowing precisely what your next move will be.

GOALS

A goal consists of setting up measurable and obtainable investment benchmarks.[193] The goal requires developing a process or set of steps to reach those benchmarks. The first piece of what encompasses an investment goal is the **objective**. Our crypto asset investment objectives can be anything, but defining your objective brings clarity. The following are examples of objectives you could have with cryptocurrency investing.

- Diversify a portfolio to include a high risk/high return asset class as a small percent of the portfolio's composition
- Increase your portfolio's alpha (return) in comparison to the S&P 500

- See an increase of x.xx percent from your initial capital investment
- Increase net position by $xxxx.xx
- Buy a new car
- Retire two years sooner

Your objective does not necessarily need to be entirely covered by your investment into crypto. Maybe your objective is to have your investment in crypto pay for 50 percent of a new car, 20 percent of a new business, or help you retire two years early. Objective setting gives us the long-term vision of what we are trying to obtain. You can be aggressive or conservative with this objective.

The second element of a goal is the **time horizon**.[194] How soon do we want to achieve our goal? It is important to give yourself an overarching timeline. Be realistic with your time horizon. Your time horizon and objective cannot be unachievable fantasies. Realism does not mean we are surrendering our goals—it means we understand that in order to achieve large goals you must execute realistic goals under realistic time frames. If we exceed beyond that, great!

The third element of a goal is the **savings rate**, or total entry point.[195] In simplified terms, how much money are you willing to invest? If you have a portfolio of many different assets (real estate, stock, bonds, etc.), deciding on a percent of your portfolio that will include the new asset is a healthy practice. This gives you a target for how much you are willing to invest. A 2 percent asset allocation of an investor's portfolio may mean they are willing to invest $60,000 or $200 into cryptocurrency. It all depends on how much capital you are working with.

Typically, as investors experience success, they will feel compelled to increase the amount of capital they have devoted to the investment. This is human nature. While this is not necessarily a bad thing, you

need to be extremely cautious about overextending your position past what is considered safe and consistent investing. If you continue to overextend (suddenly your investment makes up 40 percent of your portfolio instead of 2 percent) then you are gambling—plain and simple.

A signal that you are overinvested into a risky asset and have not diversified your risk enough is if your everyday lifestyle and well-being is negatively altered because of the risks you are taking with your investment. Journaling, once again, is an excellent signal for spotting this.

How do we go about investing our capital once we have decided how much we are willing to allocate to an investment?

Dollar-cost averaging is a useful starting method. Instead of trying to time the market, you instead decide to have periodic payments (say, one hundred dollars every two weeks for an entire year) into an investment.[196] This helps "cost average" your investment to a reasonable price point—toning down the effects of volatility.

Here is an example:

- Week 1: Purchase one hundred dollars' worth of Bitcoin for the current price of $8,000 (0.0125 Bitcoin)
- Week 2: Purchase one hundred dollars' worth of Bitcoin for the current price of $6,000 (0.016 Bitcoin)
- Week 3: Purchase one hundred dollars' worth of Bitcoin for the current price of $2,000 (0.05 Bitcoin)
- Week 4: Purchase one hundred dollars' worth of Bitcoin for the current price of $1,000 (0.1 Bitcoin)

When the price of an asset decreases with dollar-cost averaging, you end up purchasing more "shares" of the asset with your predetermined fixed sum of money. When the price increases, you

end up purchasing fewer shares. With this example, your average purchasing cost and breakeven point is at $4,250 calculated with ($8,000 + $6,000 + $2,000 + $1,000)/4 or 0.1785 Bitcoin purchased in total. If the price goes above $4,250, you are making a profit. If the price goes below, you are at a loss.

Note how this is significantly different than the following:

- Week 1: Purchase $400 worth of Bitcoin for the current price of $8,000 (0.05 Bitcoin)

In this scenario, you will make money if the price of Bitcoin goes above $8,000. Because of your lump-sum purchase, you purchased 0.05 Bitcoin, which is 0.1285 less Bitcoin owned than if you had dollar-cost averaged over the course of four weeks (0.1785 Bitcoin).

With the single lump-sum purchase, you are operating at a loss if the price of Bitcoin goes below $8,000. This is why dollar-cost averaging as a strategy is amazing in contrast to a one-time entry—you don't have to try to time the market. Instead, determine the amount of money you want to invest, and do it slowly over time. You reduce your overall risk and give yourself a chance for a safer return on investment.

Another effective method is **value averaging**. This strategy aims to invest more when the price of the investment falls, and less when the price of the asset rises.[197] For example, we set an objective to increase our Bitcoin position by $500 every month using value averaging. Here is an illustration:

- Purchase 1 Bitcoin for $5,000
- Price increases to $5,100 so your position is now worth $5,100 at the end of month, $400 short of the target value
- Purchase 0.078 Bitcoin ($400 worth of Bitcoin) to achieve the goal position of $5,500 worth of Bitcoin at the end of the month (1.078

Bitcoin at a price of $5,100 is worth $5,500)

- Price decreases to $4,000 at the end of month two, so your 1.078 Bitcoin position is worth $4,312
- The net position is short $1,688 ($6,000–$4,312) of our additional $500 target position for this new month
- Purchase 0.422 Bitcoin for $1,688 at a price of $4,000 per Bitcoin
- Portfolio has 1.5 Bitcoin—net position is valued at $6,000 with the current price of $4,000

This pattern continues to be repeated in the following months. If the monthly growth of $500 is exceeded, you can be immensely happy and choose not to put in more capital at the end of the month because our preplanned growth goal was achieved.

The main goal of value averaging is to acquire more shares when prices are falling and fewer shares when prices are rising. This happens in dollar-cost averaging as well, but the effect is less pronounced. Several independent studies have shown that over multiple years, value averaging can produce slightly superior returns to dollar-cost averaging, although both will closely resemble the market's returns over the same period. The weakness of the value averaging strategy is not having the funds to properly invest during significant shortfalls. This is why having a realistic view on potential returns in conjunction with smart budgeting with your investing is critical to the success of your goals.

The third and final entry point strategy is the **lump entry** strategy. This is the most common retail investor strategy. An investor decides they like an asset, and then decide to immediately purchase it without slowly scaling into the position. As you have seen in earlier examples, this can burn an investor. If you have the patience to set your savings rate with a reasonable time horizon using dollar-cost averaging or value averaging, you reduce your overall risk. At the

same time, lump entry maximizes possible return if the price continues to go up after your purchase—you get the best possible bang for your buck at the cost of increasing your risk (probability of not achieving your goal rate of return).

I can't express this enough: enter slowly over the course of time—you will save yourself a world of pain. And if the asset is truly undervalued, you will still come out extremely profitable with much less risk incurred.

To summarize, the Goal principle is about having clear, appropriate investing objectives. This means establishing a healthy time frame with a predetermined amount of capital or growth you are willing to invest towards.

BALANCE

The Balance principle is the system of selecting and deciding on asset allocation using a diverse set of investments**.** Balance is both a mindset and a strategy that you must adopt and practice. **At the forefront of balanced investing is diversification and asset allocation—the hallmarks of professional investors.**

Asset allocation as defined by James Chen, former head of research at GAIN Capital, is as follows: *"The rigorous implementation of an investment strategy that balances risk versus reward by adjusting the percentage of each asset in an investment portfolio according to the investor's risk tolerance, goals, and investment time frame."*

In layman's terms, it's about how much capital we devote to any given asset class over a certain time frame. Because cryptocurrency is its own asset class, the principle of balance must be applied to it as an investment—same as any other asset.

I cannot emphasize enough how important it is to diversify between multiple asset classes.

Diversification is central to the balance principle and is the most important principle in investing. Other asset classes separate from cryptocurrency have proven to be consistently valuable over time, and to gamble all your capital into any one asset class is foolish. You can reduce your overall level of risk by diversifying your investment capital into multiple investment vehicles. This divergence is not only healthy, but imperative to your investment portfolio's well-being.

Here are the primary asset classes a portfolio can consist of:

- Cash
- Stock
- Bonds
- Real estate
- Gold
- Precious metals and commodities
- Alternative investments

Diversification across multiple asset classes works because a diversified portfolio has exposure to multiple different key markets—safeguarding against weak performance in any one area.[198] For you opportunists, some portfolio styles have a high risk/reward. Before I discuss simple portfolio setups, I want to briefly touch on a cryptocurrency classification misnomer.

A common misconception is that cryptocurrency falls under the category of an alternative investment. Certain cryptocurrencies can be classified as precious metals, stock, or even real estate (tokenized assets). This is a powerful potential future reality of the blockchain space that I assume will become more fleshed out as the market

regulators and blockchain developers continue to advance and define the technology.

As of right now, even behemoth entities such as the Securities and Exchange Commission in the United States don't know how to consistently classify certain cryptocurrencies! It is best to view cryptocurrency as an alternative investment that in the future may be categorized as its own asset class with a separate set of regulations and laws.

When discussing portfolio composition, the asset class allocation percentage is the bread and butter of a portfolio. How much you commit to any given asset class (separate from which investments you choose within the asset class) is what largely determines your overall risk and return.[199]

Each asset class has thousands of different investments you can choose from. Within cryptocurrency are two categories: small market cap and large market cap cryptocurrencies. Market capitalization is a rough representation of how much the market values a cryptocurrency with the total supply accounted for.

As an example, Bitcoin's market capitalization (price of Bitcoin times the supply of Bitcoin) is $117,810,000,000 at the time of writing this. Bitcoin has the largest market capitalization of any cryptocurrency. This contrasts with the ninety-seventh cryptocurrency, HyperCash, whose market capitalization of $43 million. Notice how significantly smaller this market capitalization is compared to Bitcoin. There is significantly more risk in investing in a cryptocurrency with a smaller market capitalization for reasons discussed in Chapter 9: Qualitative Analysis—Risk.

This is why having a portfolio that is balanced is so important. Going 100 percent all in on an alternative investment asset class such as

cryptocurrency while simultaneously placing 100 percent of your capital into a relatively unknown high-risk cryptocurrency (below the top twenty largest cryptocurrencies) is plain lunacy. Spread your risk! Do not gamble away your financial security into a dead-end investment just for the one-off chance to significantly grow your wealth.

"Do not put all your eggs in one basket."

—WARREN BUFFETT

SIMPLE PORTFOLIOS

An infinite number of portfolio compositions exists. This section will cover two: aggressive and defensive portfolios.[200] These are illustrations designed to give you a picture of what diversifying means. Because the process of designing your portfolio is the primary component of achieving excellent return, I recommend investing a significant amount of time researching this topic.

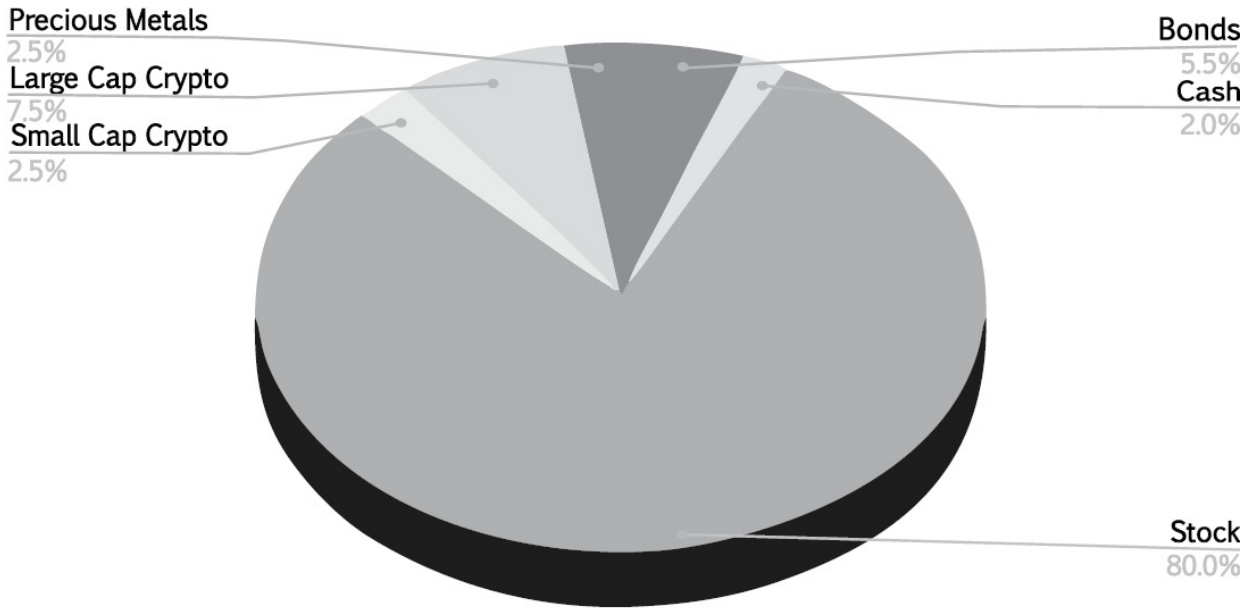


Figure 11: Aggressive Portfolio

This is an example of an aggressive portfolio. The aggressive portfolio has a high growth potential, with 10 percent being the largest percentage of allocation any investor should be willing to put into cryptocurrency. Note that even with the most aggressive portfolio, only 2.5 percent of allocation is devoted to small cap cryptocurrency—the highest risk investments (and highest potential return) assets you can possibly invest into.

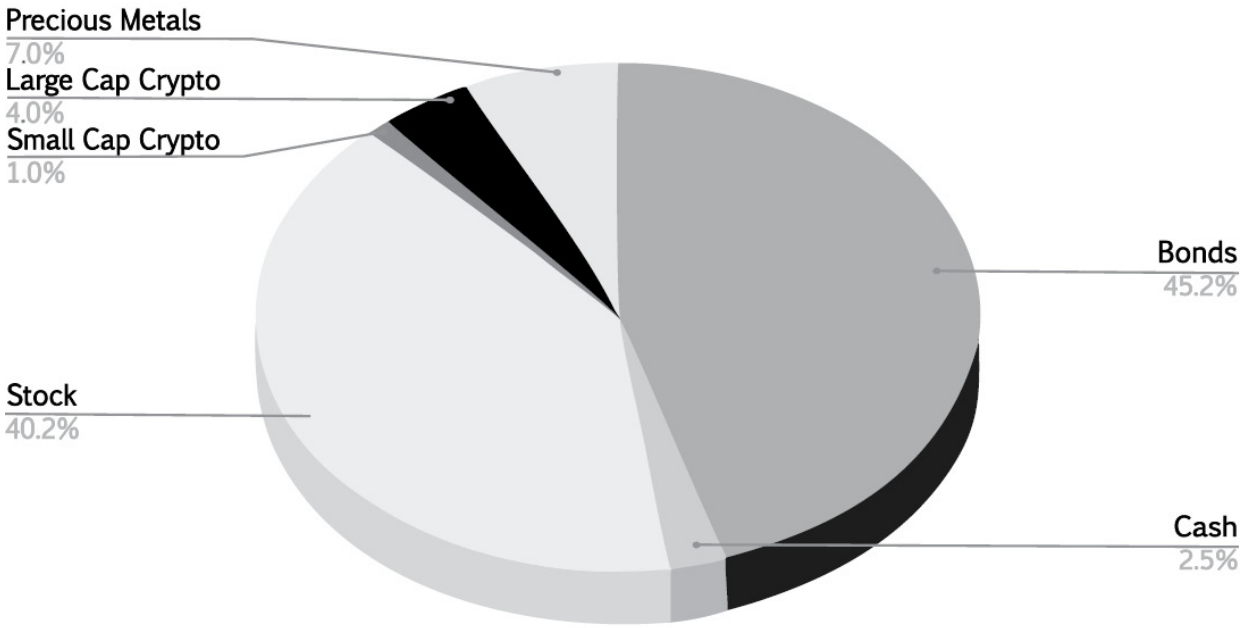


Figure 12: Defensive Portfolio

The defensive portfolio is the absolute inverse of the aggressive portfolio. The defensive portfolio is a great portfolio setup for a beginner investor that wants to get their feet wet safely and smartly in the crypto markets. Not only that, but this is a great portfolio in general, and I would recommend this style of portfolio for risk-averse individuals. The defensive portfolio's goal is to be resistant to market recessions and downturns. This is done by heavily investing into value-retaining assets (bonds and precious metals) as well as investing into companies that provide necessities to the economy.

I will pause here and address the doubters. “Five percent into crypto with a defensive portfolio? Is this guy insane?” I am a firm believer that crypto has huge growth potential, and with the rest of the defensive portfolio being extremely safe, having a percentage of the portfolio in a speculative investment is a very strong hedge against the low level of risk within the portfolio. If the 5 percent crypto asset allocation performs well, your portfolio will outperform many other defensive portfolio setups that don’t include cryptocurrency. If your crypto assets do not perform well, you are worse off. But with 95 percent of the portfolio dedicated to value retention, perhaps it is a risk you are willing to take.

You have so many options for portfolio composition—planning how you want to allocate is, in my humble opinion, extremely fun! The general consensus is that the younger you are, the more risk you can take on and be fine in the long run, as your portfolio will recover from market downturns more easily and still grow. As always, I would encourage you to err on the side of caution. As long as you diversify and don’t invest too much of your investment portfolio into high-risk assets such as cryptocurrency, you put yourself in a great position to grow your wealth.

Balance in investing is king, so don’t go chasing queens.

COST

The third principle we can control is **cost**. When we talk about the cost principle, the foremost variable that you fully control is your expenses. Entry and exit points also fall under this category, but you do not have control over the price (in stark contrast to fees). Thus, controlling fees incurred falls under the principle of cost because you have control over this variable.[201] Fees are incurred for buying, selling, and moving cryptocurrency.

Simply put, if you are putting in $100,000 over the course of two years, you want to aim for the cheapest fees for on-ramp fiat exchanges, trading platforms, and crypto brokers. This seems like a no-brainer, but often people do not hunt for better exchanges/brokers because they are intimidated by the search. Higher fees are usually associated with ease of entry. Exchanges that make it easy to deposit fiat and immediately purchase crypto with USD will often have higher fees. This could also be related to the fact that exchanges with flashy user interfaces, customer service, and simple registration processes have a larger clientele and therefore get away with charging higher fees.

Coinbase is the easiest exchange for anyone to use to purchase cryptocurrency with USD. **If you are a beginning investor, this is the go-to exchange.** Coinbase has a simple user interface, great customer support, and excellent banking relations. At the point you start investing more frequently, it would be best to look for an exchange with a cheaper fee structure than Coinbase (aligning with the cost principle). Some alternative on-fiat ramps are Gemini, Kraken, and Binance.

In summary, always look to cut costs where you can. It is one of the few things you can truly control.

DISCIPLINE

The fourth and final principle of investing is **discipline**. Unfortunately, every single self-improvement guru and fitness magazine spams this word in our faces all the time. Here is the truth: real discipline doesn't pick and choose. Discipline does not choose to follow a solid game plan one day, only to ditch it when it gets slow or boring.

You need to embrace the fact that real discipline is cold, relentless, and unforgiving. Real discipline is the antithesis of the twenty-first century attention span. Discipline is the never-ending process of steadily committing yourself to a plan by taking the right small steps over the course of the marathon that is your long-term goals. Of all the principles, discipline is the one that is the most vital to your investing success.

Fully-developed discipline is like breathing—you don't have to think about it. Discipline in its purest form is in and of itself not fun. What you derive because of discipline is fun. Investment journaling weekly takes discipline. Not jumping ship every other week takes discipline. Not switching up your asset allocation after a month takes discipline. The grass is always greener on the other side, so have conviction about your decisions and **stick with them.** That is how you develop discipline.

Discipline in investing primarily manifests itself in three ways:[202]

1. Refusing to "chase" gains
2. Rebalancing an investment portfolio when one part over-performs or under-performs beyond a preplanned percent
3. Sticking to your money allocation plan (no impulse purchases after already purchasing x amount with a predetermined sum of money)

Sounds simple enough right? If only it were so easy.

Rebalancing a portfolio is done far too infrequently by the average investor. Here is what it looks like to rebalance. Our starting portfolio is worth $1,000 with **all our asset classes' value adding up to 100 percent of the portfolio worth.** Six months went by. Our large cap crypto currency exploded in value during this time.

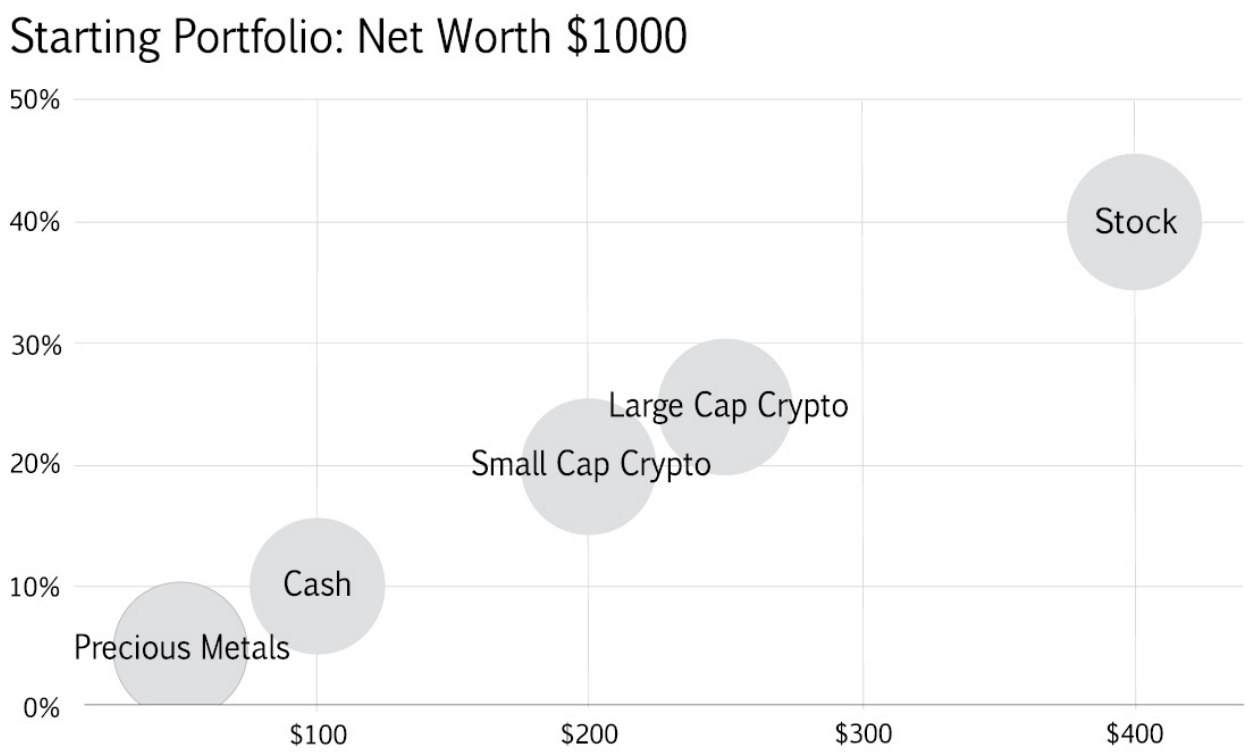


Figure 13: Starting Portfolio

When we viewed our portfolio at the end of the six months (listed below), all our assets' net values stayed the same except large cap crypto. It went from $250 to $600. That is amazing growth! Notice how different the allocation graph looks compared to where the portfolio started six months ago. This is because the large cap crypto position now holds a larger percentage of the total portfolio allocation. Even though the other assets did not gain/lose value, their percentage of allocation decreased because of large-cap crypto.

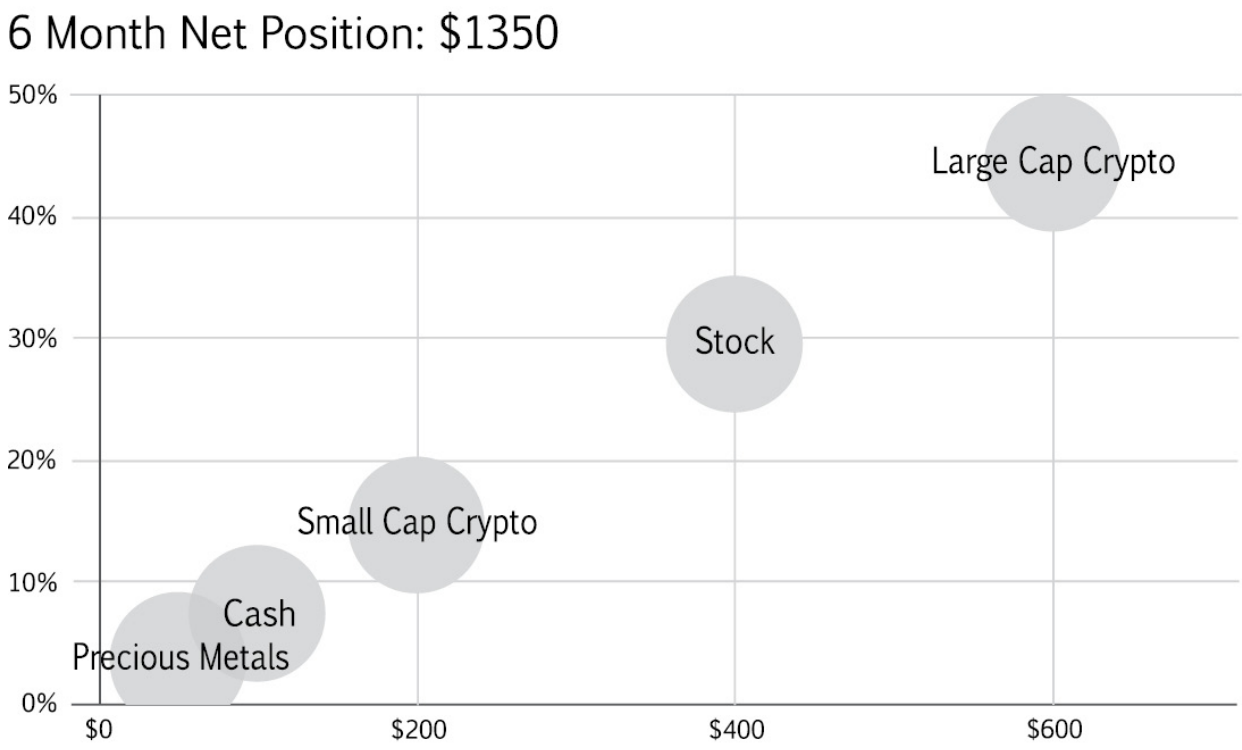


Figure 14: Portfolio After Six Months

A lot of new investors will forget to rebalance their portfolio back to their initial asset allocation composition. Because riskier assets do not retain value as well (because of greater volatility), if you do not rebalance your portfolio then you are at risk of not truly locking in your gains. The best way to move forward would be to sell $262 of the large cap crypto position and simultaneously purchase larger positions in all the other asset classes until we return to an allocation composition for each asset class roughly similar to where we started.

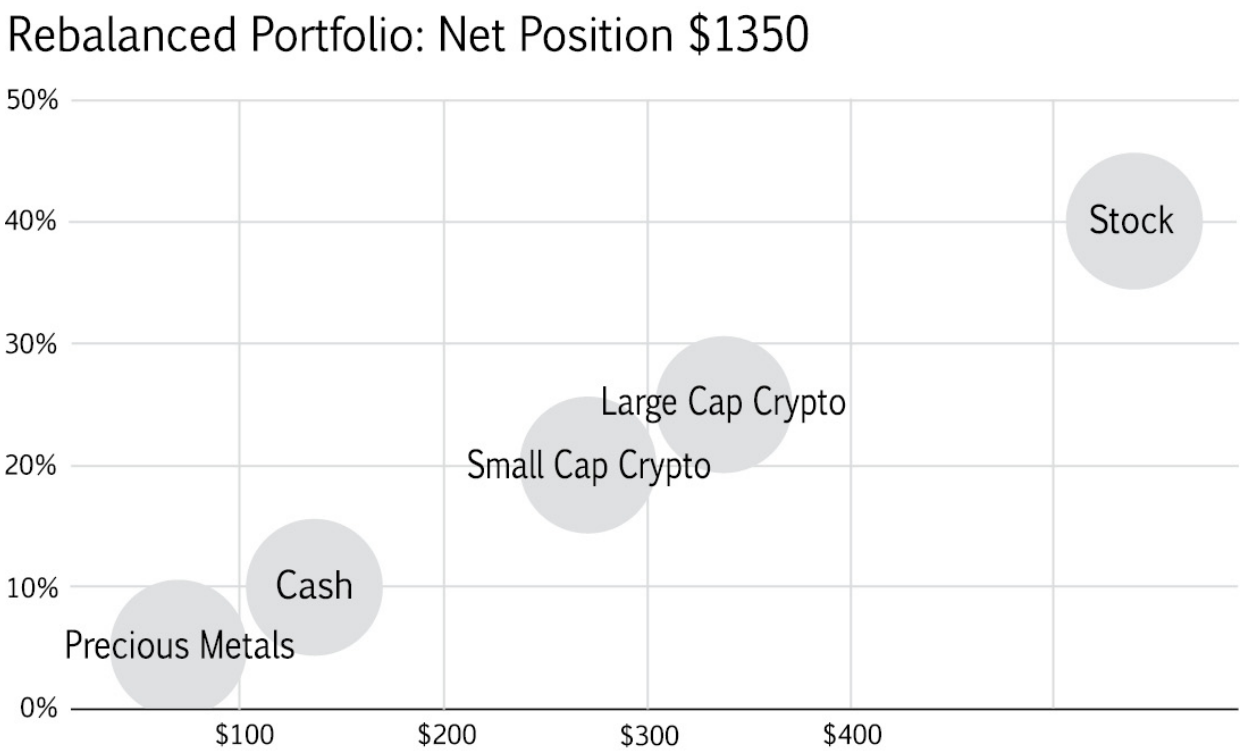


Figure 15: Rebalanced Portfolio

After rebalancing, the structure of the portfolio is back to our original asset allocation percentages and simultaneously our total net position total value has grown to $1,350 from $1,'000! This is what it means to rebalance.

The trade-off to rebalancing is it conflicts with the cost principle. The more often you rebalance, the greater the fees incurred from buying and selling fees. Professional investors set a percentage of tolerance they are willing to allow their portfolio composition to change before rebalancing. The greater the flexibility, the fewer fees incurred. The trade-off to more flexibility is that greater risk is incurred, assuming a deviation from your original portfolio composition represents risk.

Constantly rebalancing based on goal portfolio distribution can kill net position growth potential.[203] Instead, have a disciplined mindset about not letting an asset class of your portfolio exceed plus or minus

3 to 10 percent from its original allocation. Ideally, you want the changes in your portfolio composition to guide your decisions. **Portfolio composition changes should prompt questions in your investment journal**; valuable insight can be gained by digging into the "why" of significant portfolio changes.

Rebalancing requires the discipline to consistently face your investment reality and to make changes even in the face of overwhelming success. Rebalancing is the discipline of not getting too caught up in what could be a temporary success of any single asset class. The discipline to safeguard your investment portfolio by consistently rebalancing will increase your total net worth in the long run as you reallocate growth to safe value holding assets through the act of rebalancing.

Finally, sticking to your spending plan is the ultimate act of discipline. I have been in the room with people who under-planned, under-researched, and were ill-advised to purchase stock and crypto after having put in their "limit" for the month during the previous week. They do this again and again until their everyday life is suddenly affected by not having enough fiat in their bank account.

Overinvested, they are emotionally affected and proceed to make even more significant unplanned financial actions. This is terrible and can lead to life-changing financial instability.

Principles are the building blocks of our investment decision-making. Embrace them. Strive to understand and improve your long-term plan, asset allocation strategy (balance), cost minimization, and your investment discipline.

By now, you are probably itching for cold, hard numerical strategies. Abstraction is important and allocation is essential, but identifying excellent investments within any asset class (in this case

cryptocurrency) through qualitative analysis is the bread and butter many investors are familiar with. Now is the time to talk about the fun part of investing.

You're in a room with two hundred people of whom you know nothing about. Ten of these people will make you rich, and most of the room will make you poor. How do we go about sleuthing our way to success? What questions do we ask? **This is the art of qualitative analysis.**

---

191 "Vanguard Principles for Investing Success," Vanguard Investing, 2017.

192 Thayqua, "Warren Buffett: How to Pick Stocks & Get Rich (1985)," January 16, 2018, Video, 6:28.

193 Ibid.

194 Ashley Chorpenning, "Why Time Horizons Matter in Investing," *SmartAsset*, January 8, 2020.

195 Jim Chappelow, "Savings Rate," Investopedia, March 10, 2020.

196 Joshua Kennon, "Dollar Cost Averaging Explained," The Balance, December 2, 2019.

197 Movement Capital, "Value Averaging: An Alternative to DCA or Lump Sum," *Movement Capital,* December 3, 2019.

198 "What Is Portfolio Diversification?" Fidelity, accessed June 4, 2020.

199 "The Most Important Determinant of Investment Returns," Index Fund Advisors, Inc.—Fiduciary Wealth Services, DFA Funds. Accessed February 7, 2018.

200 Stephan A. Abraham, "5 Popular Portfolio Types," *Investopedia*, April 13, 2020.

201 Ellen Chang, "What to Know About Investment Fees," U.S. News & World Report, March 3, 2020.

202 Rick Ferri, "Six Rules to Disciplined Investing," Forbes (Forbes Magazine, April 24, 2018).

203 Eric Rosenberg, "The Case Against Rebalancing Your Portfolio," The Balance, April 6, 2020.

CHAPTER 9

QUALITATIVE ANALYSIS—RISK

"Zitcoin . . . shmitcoin . . . litcoin . . . Bitcoin. . . . There are so many different cryptocurrencies to choose from, and all of them seem worthless."

If you couldn't tell, these words came from someone who was less than enthused by cryptocurrency.

Shockingly, those words came from my father.

To be honest, his comment hurt. Here I was, someone passionate about an investment that was innovative and transformative. How could he be so bold as to throw everything under the bus?

Having reflected on this encounter with my father, I realized I was interacting with someone who had made both a wise and fair point.

Anyone with decent software skills can spin up their own cryptocurrency.[204] Exchanges are happy to add these new coins to their platform—they earn money from people trading. A small exchange has no strong incentive to "quality check" projects. **Because of this simple fact, investors are in danger.**[205] At your fingertips you have the ability to invest in dead projects that have long been abandoned by software developers. Simultaneously, this vice also opens the door to opportunity. You have the ability to invest in quality projects in their infancy.

This is where qualitative analysis is vital. What questions and facts need to be examined about a cryptocurrency to determine if it is

undervalued, overvalued, or even worthless?

QUALITATIVE RELATIONSHIPS

Anyone who has ever been in a relationship knows about the concept of "red flags." Those small quirks or habits that masquerade deeper behavioral issues that won't become apparent until the person has been committed to. Investing often involves committing capital. Our goal with qualitative analysis is to uncover the red flags of an asset before you invest, not after. The more thorough your qualitative analysis, the more effective you will be at uncovering a quality investment.

Qualitative analysis is subjective analysis centered on non-quantifiable information that helps generate valuable conclusions. In the blockchain space, there are hundreds of different projects to be sifted through. How do we find the nuggets of truth? Do we care about personnel? The marketing plan? The skill of the coders contributing to a project? Does that tweet really make a difference?

Your qualitative analysis is what differentiates why you believe one project is more valuable than another. It is the gradient by which you rate a project in comparison to competitors. While quantitative analysis is based on concrete numbers, qualitative analysis is everything that is not numerical. Qualitative analysis builds a narrative that informs our decision to invest in a project.

Qualitative analysis hinges upon two ideas: risks and opportunities.[206] Blockchain protocols are software. When you invest in a cryptocurrency, you must understand the fundamental risks of software development. In addition to understanding the individual risk the software project carries, you must also understand the use cases that are enabled by the particular blockchain. These use cases

are the opportunities. Valuable use cases are the catalyst for more and more people to use a particular blockchain. **This is known as adoption, the driving force of cash flows and transactions on a blockchain.** Risks are examined before adoption (which is examined quantitatively in the blockchain sphere) because the objectivity of your investigation may be tainted if you start with the opportunities.[207]

"Throughout my financial career, I have continually witnessed examples of other people that I have known being ruined by a failure to respect risk. If you don't take a hard look at risk, it will take you."

—LARRY HITE

RISKS

The beauty of software development is that the challenges and risks of yesterday are still valid today. **Due diligence is urgently in order before you invest in a cryptocurrency—not after**. This was the most common error during the 2017 cryptocurrency bubble. New investors would invest in a cryptocurrency without understanding how the underlying blockchain protocol worked, who the programmers were, and what the timeline of the project was. Only in hindsight would these new investors "discover" bits of information that fit their narrative they would then use to defend their investment decision.

Confirmation bias took center stage, yet again.

In the blockchain space, this "buy and then justify" mentality manifests itself as tribalism. Visit any online crypto community and you will see vicious attacks against different blockchain protocols. Naturally, this is in tandem with a blind defense of the cryptocurrency said tribalistic investor has invested in.

Anthony Sassano, a longtime investor and podcast host in the blockchain space had this to say:

"Cryptocurrency naturally lends itself to tribalism. There is a strong incentive to be loyal to certain projects; that incentive is, mostly, monetary. People who have invested money into something will obviously have a strong inclination to ensure its success. Of course, money isn't the only incentive people have. Strongly-held beliefs and ideologies play a huge part in cryptocurrency just as it does in real life. Some people don't even care about money, but they still want to see a certain project fail because they believe that it deserves to."

To simplify this further, **people will defend what they have invested in because they are also emotionally invested.** Be humble enough to understand that your qualitative narrative could be wrong (or at least pieces of it). If you fail to accept this, then you are no longer an objective investor. Such religiosity about your own narrative is fraught with financial risk.

What are the risks of software development? Starting in the early 1980s, a variety of in-depth studies from software engineering research tackled this question. At the International MultiConference of Engineers and Computer Scientists in 2011, Tharwon Arnuphaptrairong published a paper titled "Top Ten Lists Of Software Project Risks: Evidence From The Literature Surveys."[208] This brilliant research paper took an amalgamation of other research papers and boiled this heap of data down into a subset of risks that are commonly found in industry. Here are the four primary risk categories:

- User
- Requirements
- Project Complexity

- Team

USER

An empty parking lot at a restaurant is typically a sign of a dying or dead business. Blockchain protocols are no different. The primary risk of any blockchain resides with the user.

Imagine a road with a toll booth. In order to use the road, you have to trade in dollars for a different currency. How much you are willing to pay for the other currency in order to use the road is based on how much you value the ability to use the road.

A cryptocurrency with no users or transactions implies no one values the ability to drive on the road. Zero transactions reveal that no one cares about changing, updating, interacting, or sustaining the underlying blockchain ledger. Therefore, the cryptocurrency is useless.

If we want to invest in the most valuable blockchain "road," we must ask ourselves what factors make a blockchain less valued by users? Often, it has to do with the drivers on the road themselves. With blockchain software development, the drivers on the road are simultaneously investors. This means the drivers' visions for the what, when, and how of the road can conflict with the construction team (software development team) and fellow drivers.

The following are the most common user conflicts during software development or "road construction":[209]

- Users resistance to change
- Conflict between users
- Users with negative attitudes toward the project
- Users not committed to the project

- Lack of cooperation from the user

You currently use a toll road that brings you from A to B. You hear about a different toll road that does the same thing, but with a different design and rules. Is it worth transitioning over?

Users' resistance to change is founded upon the following question: "Is the problem solved with this blockchain worth it for me to migrate from a current (usually centralized) solution?" Finding the answer to this question should be the *first* qualitative step of any cryptocurrency qualitative investigation. A blockchain that is not solving a problem worth solving is bound to fail in the long wrong. Why switch toll roads as a driver if I am perfectly content with the toll road I currently use?

Imagine you invested in the toll road at the earliest stages of construction. You ask the construction team (software developers of the blockchain protocol) about how things are coming along. You get no response. Upon further investigation, you realize the construction crew is ignoring any and all interactions about the road. Worse, you are unable to communicate with your fellow drivers and investors because, in this fictional world, there is nowhere to meetup.

Traditionally, a specific forum exists (separate from social media) where users can ask questions and discuss the project in depth with fellow users. **If this forum does not exist, then you should not invest**. This implies a lack of a dedicated channel for developers, users, and builders to communicate with each other about the details of the project.

If the forum does exist and users are asking developers the hard questions and getting quality responses, you have found a set of developers that are addressing the central risk of a project—the

quality of communication with users about the software development and the features enabled by the blockchain being built. Users should be kept up to date on how the project works, why certain features are being put into place, how those features impact them, and how the users can help the project grow.

The reasons users would not be committed, why they wouldn't cooperate with testing, and why there may be conflict between users (with a negative sentiment about the project) can typically be traced back to the quality of communication. Therefore, you must investigate this dynamic, as communication is profoundly wrapped up in user risk.[210]

"Let the builders build and the community manager communicate" is a common phraseology and excuse used by a variety of teams building out a blockchain. In my humble opinion, this creates direct friction with users because of the fact that **users in the blockchain space are categorically expecting a quality of communication that falls in line with what a traditional stock investor would receive.** Because of the lack of regulatory communication required for any blockchain development project (and therefore cryptocurrency), there are an untold number of scenarios in which investors have put in millions of dollars, only to receive zero communication from the developers.

In the traditional stock world, this is unheard of. Investment policy statements, board calls, quarterly news releases, and investor conferences are the norm. Contrast this to crypto, where communication appears to be an afterthought. This is why user risk is the primary qualitative risk. Expectations are high because users are monetarily invested in the project and expect a certain amount of confluence on a regular basis.

Your qualitative analysis should grade user risk on a scale of zero to one hundred. One hundred would imply the best blockchain development project in the entire crypto space as it pertains to user relationships and communication. In other words, user sentiment is exceedingly positive and sustained. Zero would be the exact inverse. It would be recommended to record this entry in your investment journal—justify the value assigned and what factors it was built upon. This methodology will be repeated for all five software project risks.

REQUIREMENTS

With software development, requirements are the benchmark by which progress is measured.[211] These requirements created by blockchain software developers are the features required in order for the blockchain protocol to satisfy the goals of what said blockchain exists to solve and create. An excellent blockchain protocol will have developers that understand proper requirement creation and completion. A blockchain project that does not manage requirements in a consistent manner raises a red flag. The following are requirements risks:

- System requirements not adequately identified
- Unclear system requirements
- Incorrect system requirements
- Continually changing requirements

All projects should have a timeline of software development benchmarks and releases. This should include past releases as well as future releases.

If there is no timeline and only cryptic statements about when and how the blockchain project will be developed, then you have

encountered a monumental deal-breaker.[212] If you cannot find the history of the requirements that have been developed to date and where the project is headed with precise goals, dates, and objectives, then the underlying crypto asset is carrying a significant amount of requirements risk.

A project that has no listed requirements or evidence of software development are what we call "vaporware." That is to say, the blockchain of the project does not exist in any meaningful form, and so the cryptocurrency of said blockchain will never be of any significance.

Continually changing requirements are what I call "The Runaway Train." **This risk is the most complicated of the four requirement risks because it can be dressed up and disguised as progress.** Set a deadline, miss the deadline, and then move the deadline with a promise of "soon." Rinse and repeat. While "The Runaway Train'' isn't terribly hard to spot, it's hard to identify a project as such without sticking around long enough to see if this is true.

GitHub is a platform that hosts software projects—useful tools are available to track a project's progress. Any changes to the codebase are recorded and visible for all to see. This is where checking GitHub repositories for a blockchain project becomes a helpful qualitative hint about how a project is progressing.

Search "Official (insert blockchain you are investigating) GitHub repository." Check the open-sourced repositories and look at the progress in recent history.[213] A Runaway Train will not have any new commits, edits, or comments in recent history. If edits exist, they will be extremely minute changes that are not actually moving the project forward, creating a mirage of forward momentum.

Examining requirement risk allows you to peer into the progress a blockchain development team is making. Great progress will increase the value of the underlying cryptocurrency and give you hard evidence of the actionable steps and plans that are being made.

PROJECT COMPLEXITY

Project complexity risk is centered around the degree to which the innovation of the given project is unprecedented and groundbreaking.[214] **With blockchain, all projects suffer from project complexity risk.** As an asset class, the technology is immature, and the innovation groundbreaking. Not all blockchains are created equal, nor is the significance of the research to enable certain features and use cases. The following are project complexity risks:[215]

- Project involves the use of new technology
- High level of technical complexity
- Project involves the use of technology that has not been used prior to the project
- Immature technology

Typically, projects that incur a high degree of project complexity risk don't meet deadlines and are typically holders of vaporware. More importantly, the marketing surrounding the blockchain will give off the "vibe" of a research project. A strong clue is that the focus of the software development/marketing is centered on research instead of the adoption of the platform by users and developers. Usually these blockchain research projects do not have a usable platform or even a portion of a "toll road" to be used!

Entirely avoid the cryptocurrencies of these blockchains until there is an actual working product.

RChain was founded during the ICO mania in 2016. RChain was a blockchain project that promised to use "rho-calculus" to solve Ethereum's scaling problems, allowing more people to drive on the "toll road."[216] Rho-calculus was apparently cutting edge, but a short amount of qualitative research would have revealed it was an entirely theoretical field of mathematics that was largely unexplored.

RChain, after its ICO, a digital fundraising/stock distribution process enabled by blockchain, proceeded to burn through $65 million in runway in less than a year, buying assets such as housing for its employees. As you can probably guess, RChain is now largely insolvent.[217] A simple qualitative investigation would have pointed to a terrifying amount of project complexity risk—an entirely new type of mathematics was required in order for the project to succeed.

Rchain's narrative was entirely centered on its ongoing research—research that is not complete is just that.

Incomplete.

TEAM

"You know, as most entrepreneurs do, that a company is only as good as its people. The hard part is actually building the team that will embody your company culture and propel you forward."[218]

—KATHRYN MINSHEW, THE MUSE

A blockchain's value is built upon the skill of the individuals building the protocol in parallel to the project's ability to convey what problem is being solved and why. If I give thirty wrenches to thirty birds, they will only manage to stare at my car, or even worse,

manage to defecate on it. Give a mechanic one wrench and you have a whole different story.

The following are team risks:

- Inexperienced team members
- Team members lacking specialized skill required for the project
- Unstable organizational environment
- Level of decision friction caused by quantity of developers
- Business structure of the team

The quality of the developers is everything. Your qualitative analysis needs to ask the following question: *"Are the developers and non-developers competent/skilled/experienced enough to push the project forward to complete the goal requirements?"*

The quantity of software engineers does not always directly equate to cost-effective project progress.[219] The average amount of capital generated by ICOs was $11.2 million as tracked by coinist.io in 2019 to 2020.[220] This number has decreased since the peak ICO hype. Previously, this number was closer to $25 million—leaving business management with over-enthusiasm for what was possible and a pressure to perform.[221] Gut reactions were often to hire a large number of software engineers. While new ICO funding appears to be slowing down, the remnants of many large and mismanaged ICOs still prowl around.

Due caution is always in order. The greater the number of developers, the longer it takes for minute protocol changes to be proposed and effectively implemented into a decentralized blockchain protocol because of administrative bloat. This is a risk that large-scale projects suffer from regularly.

Within this equation is the fact that a skill labor shortage exists within blockchain development.

"In the current market, finding and retaining blockchain talent is one of the most challenging things for any blockchain company. . . . We recognize that there is a talent deficit across the blockchain industry. . . . The number of blockchain companies arriving compared to the relatively low number of those with skills or experience in blockchain is clear to see."[222]

—GAURANG TORVEKAR, CEO AND COFOUNDER OF INDORSE, A DECENTRALIZED SOCIAL NETWORK FOR PROFESSIONALS

The more high-caliber talent gathered around any given blockchain, the higher the probability the project is valuable and will go the distance. Developers are the lifeblood of a project. Competitive advantages in the blockchain space are from creating properties attached to a blockchain that are valued by users globally. This creative process and innovation are only made possible by software engineering talent.

"Companies want to have a first-mover and competitive advantage through blockchain technology, and it is much better for them to be trailblazers than play catch up"[223]

—GABRIELE GIANCOLA, CEO OF QIIBEE, A BLOCKCHAIN-POWERED LOYALTY ECOSYSTEM

Qualitatively, investigating a blockchain project's employees is important. How skilled are they? How long have they been in the crypto domain? What are their qualifications? This investigation starts with the project's website—followed up by in-depth LinkedIn searches.

Predatorial blockchain projects that are not aiming for long-term sustainability and return for the original investors will not have workers who are qualified or public facing. Workers who are here for the long term are typically blogging, tweeting, and—dare I say—loving this space on a semiregular basis. This is not to say every project needs its developers shouting from a social media platform. Rather, they should have a degree of past material created by them that points to the fact they are passionate about blockchain technology.

If a critical business entity within a blockchain project is not willing to stake its reputation in a publicly facing manner in any capacity, then the cryptocurrency of the blockchain being investigated doesn't deserve your investment trust. This reinforces what we know to be true: communication is healthy.

Leadership turnover creates a risk of an unstable organizational environment. If the original creator of a project abandons a ship without an explanation, then you may have observed a train run amok. Blockchain brings a unique conglomeration of philosophy, technology, creativity, and vision when a unique blockchain is "created" in the form of a white paper—the original outline for what the blockchain exists to solve.

When a captain flees their own proverbial blockchain ship, users will follow suit. Technology innovates at an exceedingly faster pace than traditional products. If a leader sells all their cryptocurrency of the blockchain that they created, you need to immediately re-assess your position. This sell-off is equivalent to someone selling off all their shares (ownership) of a stock. If an individual who has the greatest amount of information about a project bails, something is going on that you cannot ignore.

The final team risk is business structure: "Is the project marketing more than it is building?"

A blockchain's value proposition is weaker long term with blockchain companies that are investing more in making the product **appear valuable** as opposed to **making** the product valuable. Check for employee titles on the project's website to get an idea of the overall composition of total marketers, business personnel, and software engineers.

"Competition is fierce in the Blockchain space, for every legitimate project that exists, you will find at least ten others that claim to offer it in the future, creating more competition in your niche market. . . As a co-founder of a project, I've seen many projects make empty promises and that have had huge followings, quickly revealed as exit scams. If you are promoting [or investing] in any blockchain project, make sure you do your due diligence and are promoting something real."

—SEBASTIEN DIMICHELE, COFOUNDER OF SYSCOIN

INDUSTRY RISK

Industry risks are risks specific to an industry. Often, the most significant industry risks are out of a company's direct control.[224] When you drive on the road, you can't control the other drivers, although you can do your best to anticipate them.

In cryptocurrency, the following categories that are specific to blockchain as an industry are the heaviest hitters:

- Business Risk
- Exchange Rate Risk

Business risk within an industry risk context consists of factors controllable and uncontrollable by a company.[225] Examples are

bankruptcy of clients or suppliers, brand fatigue, loss of assets, consumer preferences, competitors' actions, or bankruptcy of the blockchain development company itself.

In the blockchain space, bankruptcy is a real risk. Over 50 percent of ICO projects have already shut down because of insolvency, making the underlying cryptocurrency worthless. A survey by Bitcoin.com from late 2017, in tandem with Fortune, found nearly 150 crypto projects failed before fundraising was complete, and over 276 failed after the ICO funds were raised.

Exchange rate risk is a subtle phenomenon, but **one that market movers pay close attention to.**

First, what is market liquidity? It is the degree to which an asset or security can be quickly bought or sold in the market at a price reflecting its intrinsic value.[226] In other words, it is the degree to which you can buy and sell an asset for the price you believe the asset is valued at.

Next, let's describe how trading and exchanging any asset works, while gaining an understanding of the importance of liquidity.

Meet our brilliant investors: Adam, Bob, Cat, Dog, and Eagle. Adam posts a potential sale of his Bitcoin for . Picture this as sticky notes being posted on a whiteboard with a ladder separating posted sticky note prices from cheapest to most expensive.

Bob posts a potential purchase of a Bitcoin at ninety cents. Cat decides she wants to purchase Bitcoin right this moment. Cat would like it for as cheap as possible, preferably for ninety cents. **Unfortunately, this market is extremely illiquid.** If Cat is going to purchase Bitcoin on this exchange right this instant, she will be performing a market order, and will have to purchase the Bitcoin for

one dollar from Adam instead of her desired ninety cents. This discrepancy between what she wanted to purchase the Bitcoin for and what is available for purchase on the market is called **slippage**.[227]

Dog posts two Bitcoin for sale at $1.10. Eagle posts three Bitcoin for sale at $1.20. Adam decided he wants to purchase five Bitcoin. If he performs a market purchase order, he will first purchase Dog's Bitcoin, and then Eagle's. Unfortunately, because no orders are on the books between Dog and Eagle, Adam will end up losing a potentially significant sum of money because of slippage.

Professional investors understand the analogy above is incomplete because published bid/ask spreads are available for all to see. Needless to say, exchange rate risk is the risk incurred because an order is executed at the worst-than-expected price because of discrepancies between bids (offer price to sell) and asks (offer price to buy at).

Cryptocurrencies with low volume and market cap have a higher exchange rate risk because of lack of liquidity. A big player who wants to exit a huge position will struggle to do so without losing a significant amount of money because of low liquidity. This is similar to Adam losing money because of the gaps between Dog and Eagle's posted sell prices.

Cryptocurrencies with bad liquidity are dangerous, as the cost to exit a position is expensive. **Investors want liquidity on entry and exit. Very few cryptocurrencies have credible liquidity to have low exchange rate risk.** From an institutional investor perspective, this is one of the many reasons cryptocurrency is regarded as being such a risky prospect.[228] Before you invest in a cryptocurrency, investigate the level of liquidity in the market for that token and

how that will impact investors' ability to enter and exit. Typically, the greater the volume, the greater the liquidity and the less exchange rate risk.

As the development of blockchain technology progresses, cryptocurrency as an asset class will become more mature and take on entirely new sets of risk. After you have rated all five of the primary blockchain risks (User, Requirements, Project Complexity, Team, Industry Risk) on a scale of zero to one hundred, you will have a risk profile scorecard.[229] In any investment, return is examined in relation to the risk that was taken in order to achieve the return. Return is generated from cash flows of a company (in this case, transactions to modify the blockchain ledger) that are ultimately redirected to the user in the form of a dividend or a more valuable asset pricing. Your risk profiles should be continually updated to reflect the state of your investments, causing you to make changes to your positions as new information modifies your risk profiles.

We have fully taken the time to examine the risks. Yet in order to understand if the project is a good investment, we must gain a thorough understanding of the narrative and opportunities of a cryptocurrency as an investment. This portion of qualitative analysis is what we will tackle next.

---

204 Jason Bloomberg, "Seven Lies ICO Fans Tell Themselves (And Anyone Else Who Will Listen)," *Forbes Magazine*, June 29, 2018.

205 Gareth Jenkinson, "Bitconnect Ponzi Scheme—No Sympathy From Crypto Community," *Cointelegraph*, January 19, 2018.

206 "Qualitative vs Quantitative Analysis," Investing.com, March 9, 2012.

207 Kevin Johnston, "The Concepts of Return on Investment & Risk," Small Business—Chron.com, October 26, 2016.

208 Tharwon Arnuphaptrairong, "Top Ten Lists of Software Project Risks: Evidence from the Literature Survey," *IMECS* 1 (March 16, 2011).

209 lbid.

210 Jorn van Zwanenburg, "7 Signs of Bad Cryptocurrency," *Invest In Blockchain*, November 1, 2017.

211 Dinesh Thakur, "Dinesh Thakur," Computer Notes, accessed June 4, 2020.

212 Olusegun Ogundeji, "Key Points to Watch for in ICOs," *Cointelegraph*, September 15, 2017.

213 Lauren Orsini and Code, "GitHub For Beginners: Don't Get Scared, Get Started," ReadWrite, July 26, 2018.

214 Dan Prince, "Project Complexity: What Makes Software Development Complex . . . and How Your Developer Can Make It Easier," *illumisoft*, August 8, 2018.

215 Rocio Poveda-Bautista, Jose-Antonio Diego-Mas, and Diego Leon-Medina, "Measuring the Project Management Complexity: The Case of Information Technology Projects," *Complexity,* 2018.

216 Ian Edwards, "Boom, Bust and Blockchain: RChain Cooperative's Cryptocurrency Dreams Dissolve into Controversy," GeekWire, February 28, 2019.

217 Mitchell Moos, "RChain Cooperative May Need to Liquidate RHOC Holdings to Remain Solvent," CryptoSlate, September 11, 2019.

218 Ben Fischer, "Kathryn Minshew: The 'Wizardess of Oz'," bizjournals.com, April 4, 2014.

219 Frederick Phillips Brooks, *The Mythical Man-Month Essays on Software Engineering* (Boston, MA: Addison-Wesley, 2013).

220 Maddie Shepherd, "ICO Statistics (2020): Funding, Investment, and Best ICOs," Fundera, December 31, 2019.

221 lbid.

222 Tony Zerucha, "Skills Shortage Hurting Blockchain Growth? Industry Weighs In," *Bankless Times*, April 19, 2018.

223 Tony Zerucha, "Skills Shortage Hurting Blockchain Growth? Industry Weighs In," Bankless Times, April 19, 2018.

224 Yuval Torbati, David Bodek, and Mark Puccia, "Methodology: Industry Risk," *Ratings Direct* (S&P Global Ratings, 2016).

225 Will Kenton, "The Ins and Outs of Business Risk," Investopedia (Investopedia, February 5, 2020).

226 CFI, "Liquidity—Definition, Example, Market vs Accounting Liquidity," Corporate Finance Institute, February 26, 2020.

227 Leo Smigel, “Slippage: What It Is & How to Avoid It,” *Analyzing Alpha*, November 29, 2019.

228 Caspian, “The Four Barriers for Institutions Entering Crypto,” Medium. Caspian.tech Blog, July 8, 2018.

229 Ashley Chorpenning, “What Is a Risk Profile?” SmartAsset, January 31, 2020.

CHAPTER 10

NARRATIVE

"Narrative becomes the way you make sense of chaos. That's how you focus the world."[230]

—Dennis Lehane

Every once in a while as a writer, you get pulled into writing a brief chapter—something so short and quick you question whether it should be included. This was that chapter. The pull of narrative on investing and the lack of discussion about narrative in investment literature made it irresistible for me to quickly scratch the surface of this topic.

Narrative is what average investors latch onto, whether they are aware of it or not. Let's take a look at Apple's narrative from a "simpleton" investor perspective:

"Apple is a company that is constantly innovating great electronic products I use every day. Steve Jobs was groundbreaking with his creativity and company culture cultivation—ultimately creating a company that deeply values its shareholders."

This simple narrative inspires. Apple's products give customers the ability to connect, engage, and create within the digital community. Simplicity is king with investment narrative. Apple is a prime example of reputation and quality influencing narrative.

Imagine yourself for a brief moment as a millennial who orders coffee from Starbucks every single day on the way to work. During lunch, after a load of stressful meetings, you pick up a steamy Starbucks coffee to forget the woes of employment. On the drive home you down hot coffee from a Starbucks-themed thermo cup. In your millennial mind, what better investment could you put your capital into than a company like Starbucks, which you use every day?

To you, Starbucks has friendly employees, quick service, and a product you can't live without.

That, my friends, is narrative. It is a snapshot of what we perceive the company to be. Even if narrative is truthful, **narrative is never the full picture.** Yet the power of expectations—and by extension, narrative—is a catalyst for measurable action. From an economic theory standpoint, you cannot ignore the impact of narrative because it directly impacts investment decisions.

"We relate to and remember stories better than we do numbers."[231]

—ASWATH DAMODARAN

Every cryptocurrency has a narrative, for better or for worse. **Narrative is powerful. It moves money.** The simpler the narrative, the more investors and users feel they can use or relate to the investment vehicle.

What is Bitcoin's narrative? From a simple investor's perspective, it is as follows.

"Bitcoin is the first truly digital currency that is globally accepted by any electronic device attached to the internet. Bitcoin is a digital asset that is limited in supply and fills a niche role similar to that of rare metals. It is a twenty-first century product made possible by cryptography and mathematics—maintained by thousands of computers."

Bitcoin has a more complex and less "tangible" narrative than Starbucks or Apple for the average person. Despite this contrast, Bitcoin has a far simpler and compelling narrative than the majority of other cryptocurrencies.

I've randomly selected the 114th-largest cryptocurrency using a two-hundred-sided digital die to compare to Bitcoin's narrative, once again using a narrative that appears common surrounding this cryptocurrency.

"Golem is a global, open source blockchain project that enables decentralized sharing of computer power in order to solve complex computations for an individual entity. These complex computations can involve CGI rendering, machine learning, or scientific computing. It is made up of the power of users' machines that are integrated into the network. This creates a decentralized sharing economy of computing power that anyone can access."

While Golem appears to have some intriguing utility, from a narrative perspective the story feels complex and undefined. Golem as a blockchain project appears to be for a small audience with extremely specific use cases. The utility sounds highly ambiguous —"decentralized sharing of computing power."[232]

This is borderline wizardry for the layman investor looking for a simple narrative, even if it is an excellent investment separate from narrative.

How many people are actually going to use Golem? Could I picture using this product or service daily? Ask those same questions about Apple, Starbucks, and Bitcoin, and you can easily answer with, "Yes, yes, and somewhat maybe." But with Golem, from a simple narrative angle, the project is convoluted enough so as to not encourage the same enthusiasm as a cup of Starbucks might.

Finding a simple narrative in the blockchain space might be the most important investment analysis, assuming the other qualitative pieces fall into place. Humans are drawn to stories—find the stories

the greatest number of people can understand, use, and be inspired by. That is where the greatest growth will be.

Because whether we like it or not, we invest in compelling stories.

---

230 Andrew Cotto, "A Conversation With Dennis Lehane," grubstreet, January 10, 2012.

231 Aswath Damodaran, *Narrative and Numbers: the Value of Stories in Business*, HarperCollins India, 2018.

232 "Home," Golem, accessed June 4, 2020.

CHAPTER 11

QUANTITATIVE MODELS & METRICS—ERROR OF PROJECTION

"People who watch their weight, golf scores, and fuel bills seem to shun quantitative evaluation of their investment management skills although it involves the most important client in the world—themselves."

—Warren Buffett

Numbers can be scary.

Cold.

Calculated.

Emotionless.

"Facts don't care about your feelings," and neither does quantitative analysis. Fortunately, we have *options*. No model is perfect. Every model is flawed. **The key is finding a model that lines up decently well with reality** such that when the present reality is disconnected from what we know to be true, we get to call it out.[233] Place our bets. Stare the market straight in the eye and say, "You are overvaluing this investment" or "You haven't accounted for this piece of information."

The goal of this chapter is to examine the numbers that matter. Quantitative measurements give us the ability to compare blockchains to each other, as well as make predictions and projections about the future. While some of these sections appear to be mathematically intensive, all these models are publicly available by searching "CarterLWoetzel GitHub" online—you don't have to make any of these models from scratch.[234] The purpose of each section in this chapter is twofold: explaining the underlying logic of each model in addition to giving you simple examples of each model in action. It will be up to you to utilize the resources provided on my GitHub, as well as finding other models that exist out in the wild.

In my mind, two types of models exist: traditional and weak. Traditional models generate a target price based on dividends given to the owners of an asset, such as a stock or bond. Weak models are used to estimate the value of non-dividend producing investments. In the cryptocurrency space, dividends are uncommon. This is shifting as many blockchains move to the "proof of stake" consensus model, which provides a dividend to those who "stake" their crypto to secure the network.[235] Currently, weak models are more common and accessible for cryptocurrency price projection. Regardless, we will propose a variety of models—many of which are looked down upon and others that are widely accepted.

COMPARISON METRICS

You are comparing two blockchains to each other, trying to figure out which cryptocurrency is more valuable. How do you tell which blockchain is more valuable quantitatively?

Blockchain Metrics To Compare	
# of nodes	Measures decentralization & security
# of daily transactions	Measures the use-case activity of a blockchain
# of non-empty wallets	Measures adoption
Network hashrate	Measures the amount of computation power competing to update a decentralized ledger
Daily trade volume	Measures investment activity
Total miner revenue	Measures daily revenue earned by miners
Total inflation rate	Measures coin distribution growth rate

Figure 16: Comparison Metrics

As mentioned earlier, Coinmetrics as well as Blockchain Charts have all of this data publicly available. Marketing and PR can't hide from these quantitative comparisons between different cryptocurrencies. Number of nodes is especially important because the more

distributed the network, the safer the network is from 51 percent attacks, censorship, and network downtime. If a blockchain network is doing better on all of these metrics and is less valued than a different blockchain, it is a strong signal it is undervalued.[236]

NET WORTH MARKET CAPITALIZATION MODEL

The "Net Worth Market Capitalization Model," created by Daniel Sangyoon Kim, is **based on the assumption that in the near future, crypto will be part of every wealthy American's portfolio**.[237] This weak model is not based on dividends, but a qualitative prediction based on cryptocurrency's relevance as an asset class.

Network Capitilization Model	
Projected cryptocurrency market capitalization	M
Net worth of investor group	η
% of total portfolio invested into crypto for each invester	P
% of total market share of examined cryptocurrency	S
Total Currency In Circulation	C
Network Capitilization Model Equation	M =η * P *S
Model Target Price	M / C

Figure 17: Network Capitalization Model

Here is a simple example using Bitcoin:

- Projected 0.025 percent of American's portfolio (in the top 1 percent of income) will invest in cryptocurrency
- 1.3 million households in the top 1 percent account for $11 trillion
- Bitcoin holds 50 percent of the total cryptocurrency market capitalization
- 21 million total Bitcoin in circulation
- $5,200 current price of Bitcoin

- Projected Bitcoin market capitalization = $11 trillion * 0.025 percent * 50 percent = $137.5 billion
- Projected Bitcoin price = $137.5 billion / 21 million Bitcoin = $6,547
- Projected Bitcoin price $6,547 > current Bitcoin price $5,200

Because the projected value is greater than the current price, this quantitative model gives you a target sell price of $6,547 (a 21 percent return on investment). Kyle Samani of Multicoin Capital makes an argument for a projected $50–$100 trillion case in net worth invested based on Bitcoin use cases as digital gold, Bitcoin deflating the monetary premium of a variety of assets, Bitcoin as a replacement for offshore bank accounts, Bitcoin as a means for securing the world's assets, and new economic activity facilitated on the Bitcoin network.[238]

I hope the error of prediction is evident in this kind of model. Yet this model holds some truth: a certain number of people in the future will invest a certain amount of capital into cryptocurrency as an asset class. Every cryptocurrency holds a certain amount of the market share of the crypto sphere and therefore, based on the total capital invested into the asset class, will result in a price for every single cryptocurrency based on their respective market share. If you can have broadly accurate predictions of what these numbers look like in the future, you can make decisions quantitatively right now—radically error prone, but slightly helpful.

INDUSTRY SHARE-STEAL MODEL

A weak model I have created is built on the idea that a blockchain and its respective cryptocurrency will gobble up a certain amount of a market share based on the use cases enabled by the blockchain. The benefit of this model is that it creates a logical ceiling or floor on valuation.

Take NEO, a cryptocurrency that aims to be a peer-to-peer digital currency aiming for cheap fees and a better smart contract design than Ethereum.[239] Because the NEO blockchain is largely focused on transaction facilitation, we can somewhat fairly compare it to a company such as PayPal.

NEO has approximately eighteen thousand transactions per day.[240] Compare this to PayPal, which has five million transactions per day.[241] We will calculate NEO's "stealing" of PayPal's market cap based on the ratio of NEO's transactions to PayPal's transactions, which is 18,000/5,000,000 = 0.36 percent. Assuming NEO takes 0.36 percent of PayPal's market capitalization (cap) using (Market Capitalization Stolen * M) / C_c, where M is equal to PayPal's market cap ($182.02 billion) and C_c is the amount of NEO in circulation, we generate the following price:

Projected NEO Price = (0.0036 * $182,010,000,000 (PayPal Market Cap)/(100,000,000 NEO in circulation)= $6.55

Compare this to the current price of NEO of $9.55, and suddenly this model starts to give us some decent clarity. Perhaps market share use cases other than transaction facilitation account for the discrepancy. In the future, if NEO were being sold at twenty dollars while still only generating eighteen thousand transactions per day, we can firmly say we have quantitative evidence showing that the market has diverged from reality. If the market is valuing NEO drastically more without any increase in adoption (daily transactions), then we hedge our bets against the current NEO price assuming there is no new qualitative information to justify the price increase.

The much more dependable valuation of PayPal can be used as a hazy mirror to value different cryptocurrencies that are focused largely on transactions. This same process can be applied to blockchains

focused on impacting other specific industries by creating a quantitative marker based on a reliable, publicly traded stock.

Note that this same model can be used to make projections—if adoption in the future will increase NEO's number of total transactions to eighty thousand per day, suddenly the underlying valuation needs to reflect this increase in adoption. While traditional models are based on the growth of many future cash flows, weak models for cryptocurrency use transactions as the fundamental building block.

COMPARABLE TOKENS MODEL

Ernst & Young released "The Valuation of Crypto-Assets" in 2019.[242] Within this primer, the comparable tokens model is described:

" Consider the token market capitalizations achieved in recent, comparable ICOs as a proxy for the total value of the subject tokens issued, similar to the benchmarking approach taken in the valuation of early-stage companies raising VC funding rounds."[243]

Essentially, you take the market cap of the subject cryptocurrency you are examining (coinmarketcap.com is an excellent site for this), make a market capitalization comparison to another cryptocurrency, and pose the following question: "On the basis of my qualitative risk analysis and the quantitative metrics of these two blockchains, is the subject token properly priced in relation to another similar crypto asset?"

With blockchain, the comparable tokens model appears to be one of the most appealing models because it takes your qualitative investigation far more seriously than other models. So while this is about as subjective as a model could be, it is once again better than nothing. Here is an example of using this strategy:

	TRON	XRP
User	65	30
Requirements	30	90
Project Complexity	75	50
Team	90	65
Total	260	235
Target Price Growth	10.64%	~~NULL~~

Figure 18: Comparable Token Model Example

Using an extra simplified scorecard, which should include the comparison metrics listed earlier but doesn't for this example, we examine the qualitative risk scores. According to this (fictional) qualitative scorecard, TRON's market capitalization should increase by 10.64 percent because of the difference in risk, despite the fact the market does not currently price the respective cryptocurrencies this way. While this is a pretty absurd pricing model, this is surprisingly how many venture capitalists (as mentioned by Ernst & Young) operate at the earliest stages of valuation.

DISCOUNTED TRANSACTION CASH FLOW MODEL

The investment value of a blockchain is the total revenue generated by transactions, distributed to those who secure the network by staking or mining the cryptocurrency of said blockchain. Revenue is created and given to those who secure the network per transaction appended to the blockchain ledger. Every transaction is priced by a user but executed only if the miner or staker has determined the fee

that will be received is worth it in relation to their costs (electricity costs to run a node, risk, and target rate of return). If the proposed user fee is worth it, the miner/staker adds the transaction to the block of transactions that will be appended to the ledger if the cryptographic solution is found.

As such, the stakers (those who lock their cryptocurrency into a smart contract to secure the network using the Proof of Stake Consensus model) or the miners (who expend electricity to append transactions using the PoW model) are the ones who decide the baseline value of any given cryptocurrency. Note that the market buyers and sellers continue to trade for certain prices, but because the miners and stakers are the ones who generate and receive cryptocurrency for maintaining the blockchain, their valuation of any cryptocurrency carries far more clout than a trader **in the long run.**

The more people adopt a blockchain, the more transactions that are executed. As a result of more people fighting to have their transactions be a part of the most recent block to be appended to the ledger, the greater the transaction fee. This is because miners and stakers can drive a harder bargain. All of this is classic supply and demand.

My model assumes growth in average fees is proportional to the growth in total transactions on a yearly basis. This tends to underestimate average fee growth, as the spurts in demand can be very unstable, strongly impacting the mean fee price. As time progresses, total transactions and the average price will more than likely decouple as innovation in blockchain technology will aim to decrease fees, which would increase total transactions to a blockchain as it becomes cheaper to transact and use because of the blockchain design improvements.

In addition, **active currency in circulation** is the set of crypto that is being used for its intended purpose (smart contracts and transactions). Miners and stakers are only concerned with the total level of activity that generates them revenue, and therefore will largely ignore currency that sits inactive. Active currency in circulation can be hard to hunt down for smaller cryptocurrencies, so beware of the significant impact on this model if total currency in circulation is used instead.

For those of you not familiar with the traditional discounted cash flow model, doing some basic research on the present value of future cash flows might be worthwhile.[244] I will gloss over these basics for now as they are taught in a variety of courses and textbooks. The discounted transaction cash flow model (DTCF) I propose is as follows:

$$DTCF = ((T_1 * F_1)/(1+r)^1) + ((T_2 * F_2)/(1+r)^2) + ((T_3 * F_3)/(1+r)^3) + ... + ((T_n * F_n)/(1+r)^n)$$

Figure 19: Discounted Transaction Cash Flow Model

- T = Total Transactions for year *n*
- F = Average Transaction Fee for year *n*
- r = Miner/Staker Target Rate of Return

Every year, the total transactions per year and the average transaction fee per year will grow by the projected total transaction growth rate. After this summation is done for *n projected time periods,* the total discounted cash flow is divided by the total active currency in circulation to arrive at your projected target price. Note that this formula is identical to the discounted cash flow model, with a slightly different structure to reflect revenue coming from transactions and fees of a blockchain to miners and stakers.

Year	Average Transaction Fee	Total Transactions	Discounted Cash Flows
2020	$0.23	182,500,000	$39,228,971.96
2021	$0.35	273,750,000	$88,265,186.92
2022	$0.52	410,625,000	$198,596,670.56
2023	$0.78	615,937,500	$446,842,508.76
2024	$1.16	923,906,250	$1,005,395,644.71
2025	$1.75	1,385,859,375	$2,262,140,200.61

Projected Growth Rate of Total Transactions	50%
Staker/Miner Target Rate Of Return	7%
Total DCF	$4,040,469,183.52
Total Active Currency	16,200,000
Value Per Ethereum Share	$249.41

Figures 20, 21: DTCF Model Data

The 7 percent target rate of return is what is set to be in place for the Ethereum network with proof-of-stake and is approximately the rate of return miners are operating under with the current PoW consensus model.[245] The Ethereum blockchain saw a 2,500 percent increase in total transactions from 2016 to 2017.[246] This slowed down to 65 percent growth from 2018 to 2019.[247] As such, I decided this particular Ethereum price valuation should underestimate growth per year at a mere 50 percent to give a realistic picture of the next five years. Depending on this growth rate, the value of Ethereum can range quite a bit. Seventy percent growth rate in total transactions per year puts Ethereum at $732 for Value Per Ethereum “share” compared to the current price of $203 (as of writing this). In addition, the starting average transaction fee of $0.23 in 2020 also impacts the valuation significantly.

Having created this model, I can say with confidence it has plenty of errors. As with all investment models, our goal is to match the value of an asset based on quantitative metrics and future growth projections using information publicly available.

I hope you can now see how flimsy and chaotic the art of quantitative modeling appears to be.[248] As blockchains continue to mature, I expect we will see far better models appear. Cryptocurrency is a strange hybrid of currency, store of value, and digital fuel. It will power the future, that much I am certain of.

How shall we accurately measure its worth?

This remains a frustratingly complex mystery that will continue to be chipped away at as cryptocurrency sees more adoption from institutional and retail investors.

---

233 "Quantitative Analysis—Definition, Techniques and Applications," *Corporate Finance Institute*, February 19, 2020.

234 Carter Lee Woetzel, "CarterLWoetzel/Building-Confidence-in-Blockchain---Next-Steps," GitHub, June 6, 2020.

235 Binance Academy, "Proof of Stake Explained," Binance Academy, January 19, 2020.

236 Jeff Fawkes, "The 8 Most Important Cryptocurrency Metrics to Look For," Bitsonline, February 1, 2019.

237 Daniel Sangyoon Kim, "Fundamentally Valuing Bitcoin at $45,000 / BTC," Hacker Noon, May 4, 2020.

238 lbid.

239 Shobhit Seth, "Why NEO Can Do What No Other Cryptocurrency Can Do," *Investopedia*, January 29, 2020.

240 "Charts," Coin Metrics, accessed June 4, 2020.

241 Leena Rao, "PayPal Now Processing $315 Million In Payments Per Day," *TechCrunch*, September 25, 2011.

242 Ernst & Young, "The Valuation of Crypto-Assets," 2019.

243 lbid.

244 “Discounted Cash Flow DCF Formula—Guide How to Calculate NPV,” *Corporate Finance Institute,* October 22, 2019.

245 Nikolai Kuznetsov, “Ethereum 2.0 Staking, Explained,” Cointelegraph (Cointelegraph, May 25, 2020).

246 “Ethereum Transactions Per Day:” YCharts, accessed June 4, 2020.

247 lbid.

248 Sheba Karamat, “How Are Crypto Prices Determined?—Cryptocurrency Guide,” Coin Rivet, March 23, 2019.

CHAPTER 12

ENTRY & EXIT

Entry is permanent. There are no take backs. People often pose the question, *"When do I exit? When do I sell an asset?"*

This seems to trouble them deeply. They torture themselves over a decision that was largely decided when they made a decision to buy.

The first foundational purchasing rule of thumb that I want to drill into your head is that your entry purchase price is exponentially more important as a decision than your exit price. Anyone can strategically plan their exit based on how the market decides to move. The true skill lies in anchoring your entry into a position where loss is unlikely and profitability likely.

No guarantees exist.

No one promised you universal success with entering and exiting a position, and if they did, they were lying. Here is the truth: what I tell you comes with zero guarantees. The market ultimately decides price movement and the valuation of any given asset. You don't control the market. You are simply trying to figure out where the consensus of an asset will be in the future compared to now, and if there is a discrepancy the market has not yet factored into the price.[249]

Here are the three assumptions I will make when investing in an asset:

1. You believe the asset is undervalued under some time frame

2. You believe the asset's price evaluation will eventually reflect this under evaluation over the course of a certain time frame because of information (from your qualitative or quantitative analysis) that the market has not yet priced in
3. You are looking to buy and sell without leverage instruments

These simplified assumptions are established to keep things simple as we discuss entry and exit. This is not to say I don't believe in selling an overvalued asset—quite the contrary!

MEAN

Mean is the central value of a set of numbers.[250] Mean price in the market does not reflect immediate price, but it does reflect the average price valuation by traders and investors over a certain time frame. **The thesis of this chapter is that a mean is an okay indicator for an entry point—far better than using no indicator.**[251]

Price is constantly in flux trying to determine what we all agree to be the true **permanent** value of an asset. Buyers and sellers are always in disagreement on the long run, trying to find the price at which all buyers and sellers are permanently content, which is impossible. Over the course of a large data set such as two years, the thesis would hold that there is a price point that throughout the flux of agreement and disagreement is ultimately close to the theoretical true value of the present moment not yet agreed upon. It is the hidden equilibrium in the market that will never be sustained. Price will always rebound away from or toward this point because such a consensus will never be reached. This Equilibrium Mean Price Point (EMPP) is essentially a complex moving average that is tough to influence, creating an excellent indicator for entry and exit decision-making.

The implication is if you can find a price point that is within even 5 percent of this extremely slow-shifting equilibrium, you can confidently buy below this EMPP because at that point in time the market is very likely undervaluing the asset (compared to this equilibrium price point), assuming you have done your qualitative and quantitative research and are confident the asset is undervalued with regard to that analysis as well.

Note that I am not necessarily claiming the current price is "wrong." I am simply claiming that as the current set of information has shifted sentiment to the point that the market collectively agrees, the current price is what the underlying asset is worth at this moment.

But markets are finicky. Chaotic. Temperamental. **Is a market bubble an exercise in collective rational thought?** On the contrary, bubbles are the evidence that shows that markets will go mad. People can be irrational, and they can do so as a collective unit.[252]

You have the ability to make rational decisions based on historical data that give us indicators that maybe, just maybe, the market will be "wrong" on a ***different time frame***. Sometimes the best thing you can do is to make no decision at all. Your money should always be growing in some sort of investment vehicle (or else you are losing money to inflation), but if you have money that is dedicated to investing particularly to volatile assets, not making a decision can be the smartest thing to do. Standing still is a decision in and of itself, and not acting is okay.

EMPP

The goal of designing Equilibrium Mean Price Point (EMPP) was to have an indicator that keeps a beginning investor extremely grounded in reality when it comes to entry. A much more simplified

process than what is described can be found at marketwatch.com, which has the option to include moving averages on multiple time frames for any cryptocurrency chart.[253] Moving averages attempt to spot market divergence from historical pricing and do not make any projections about the future.

As a result of this conservatism created by moving averages, risk is ultimately reduced at the cost of perhaps not choosing to enter (losing out on potential gain). This is why dollar-cost averaging is my recommended entry strategy for anyone beginning to invest in cryptocurrency. While the EMPP is your sanity check, dollar-cost averaging is your risk reduction strategy for when you do decide to invest in a crypto asset because of your quantitative and qualitative analysis.

Calculating for the EMPP involves creating an average of averages, and it must be recalculated **every time** an entry or exit decision is being made.

I am not suggesting using EMPP as a day trading strategy. EMPP is an entry point indicator used as a sanity check for your quantitative model price target (created with the help of your qualitative analysis). *The value of an asset is the present value of future cash flows. EMPP cannot reflect this projection into the future, but it can warn us if the market has gone off the deep end and give us an idea if the current price is reasonably safe for entry.*

DATA AND COMPUTATION

Where does one acquire the data to compute an EMPP calculation? **Coinmetrics** (open-sourced and free to use) is an excellent site that lets you download spreadsheets of each cryptocurrency with all of their historical data for free—no account needed.[254] Using the price data of said cryptocurrency, you can then calculate for the EMPP with

some very basic Excel skills. The CSV data offered by Coinmetrics contains the following information:[255]

- Active addresses currently using the blockchain protocol
- Market capitalization
- Block count
- Block size
- Mining difficulty
- Daily fees generated
- Issuance/inflation rate
- Price
- Total current supply
- Daily transactions
- Volatility of daily returns

I would encourage you to play around with Coinmetrics. It's empowering to do so. With some basic Python coding or Excel skills you have the basis for creating your own quantitative models or comparison ratios between a range of blockchain protocols and cryptocurrencies using quantitative metrics.

Data gives hard quantitative insights. **Never underestimate what can be uncovered with this type of research.**

Returning to the process of creating the EMPP, three sets of starting dates are used to compile our sets of averages that are used to generate the EMPP.

1. Present day
2. Ninety days previous to today
3. Highest priced day in the last year

The present day is used because, clearly, we care about market sentiment in recent history. Ninety days previous to today is leveraged to account for any price trends leading to the present day,

as well as the lead up to those trends. The highest price within the last year from the present day is used to account for the data leading up to any recent bull runs. We must include volatility within the EMPP to some degree, as at these focal points in time a consensus existed between buyers and sellers that the asset should be priced at a significantly higher price than the previous historical prices.

For each starting date, you compile a set of price averages looking back into history. Four averages for each starting date are calculated using the last one hundred, two hundred, three hundred, and four hundred days respectively. Next, a mean of the four averages is generated for each starting date. Finally, the EMPP is created using the mean of all three means previously computed.

When all is said and done, the EMPP consists of three thousand data points, with heavier weight given to days closer to the starting points because of overlapping averages creating redundancy. This is intended to amplify the effect of these data points on the overall EMPP.

Here is an example of calculating and using EMPP with Bitcoin using today (2/21/2020).

Average Daily Prices	400 day avg.	300 day avg.	200 day avg.	100 day avg.	Sum of means	Mean of averages
Present day as the starting day	$7,718.35	$8,927.09	$8,910.86	$8,302.12	$33,858.42	($33858.42 / 4) = **$8,464.61**
90 days previous to today as the starting day	$6,315.03	$6,167.74	$6,971.82	$9,672.64	$29,127.23	($29,127.23 / 4) = **$7,281.81**
Highest priced day in the last year as the starting day	$5,843.54	$5,491.88	$5,285.45	$6,875.41	$23,496.28	($23,496.28 / 4) = **$5,874.07**

Figure 22: Average Daily Means

Sum of all 3 means	$21,620.48	IF (EMPP > Price) Consider Purchase
EMPP Calculation	($21,620.48 / 3) = **$7,206.83**	$7,206.83 < $9,746.00
Bitcoin Current Price	$9,746.00	Therefore, do not purchase.

Figure 23: EMPP Calculation

If the price of Bitcoin were below the EMPP of $7,206.83, then you would have a healthy indicator that now may be a good time to enter. Your quantitative and qualitative analysis are your driving forces for a decision—EMPP is merely the sanity check. The further the price is from EMPP, the more wary you should be. Clearly, if the current price is drastically different from the EMPP, then the market currently is diverging from historical pricing. You need to understand why that is, and then make a decision if you believe the market is right or wrong in the long run.

As always, dollar- or value-cost averaging is the safest method for entering consistently once you have identified an asset you want to purchase. **Use EMPP or some other moving averages as a sanity check**, and then go ahead and make your purchase consistently over a longer time range to reduce your overall risk (at the cost of potential return).

Technical analysis will attempt to coach you on spotting short-term trends to decide on entering and exiting. Personally, I believe in the power of long-term trends in tandem to the belief that consistently beating the market is nearly impossible for the average person in the short term.

EXIT

We've talked about entering, but what about exiting? A couple of options to consider exist, all with varying degrees of risk and return.

- Sell all crypto "shares" at once
- Scale out of a position quickly
- Scale out of a position slowly

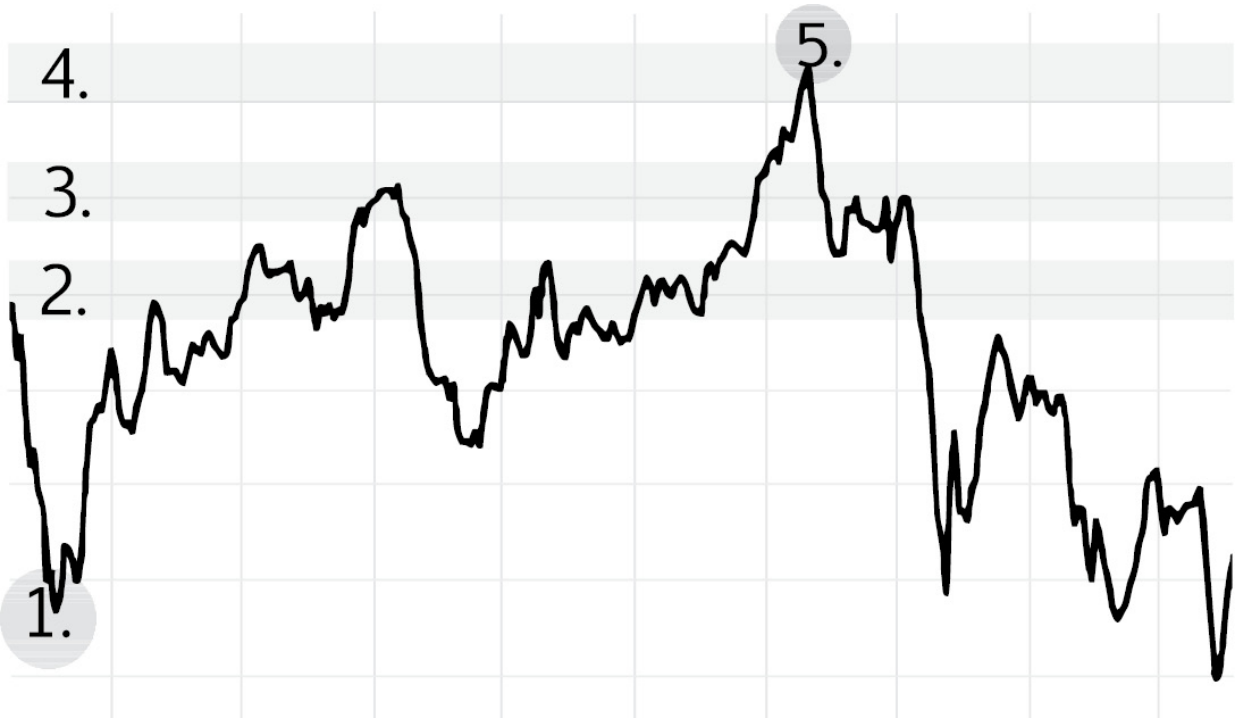


Figure 24: Entry & Exit Scenario

This chart is an excellent example of a typical entry and exit scenario. Circle 1 is where you purchased, with a target sell price at circle 5, generated by whatever quantitative model you are leveraging. Note that while you are at circle 1 when you purchase, you cannot see the rest of the chart because the future has not yet happened. Zones 2, 3, 4 are price ranges where you might look to sell a certain percent of your position leading up to your target sell price (circle 5) in order to "lock in" profit (selling at these lines are at prices higher than what you bought for, therefore generating a profit).

But how do we determine how much of our position we want to sell at any given price? Do you sell all your cryptocurrency at zone 2? Only 10 percent of your crypto? As you can imagine, infinite ways to exit a position exist. Thus, we will return to our three original ways to exit: all at once, quickly, and slowly.

ALL AT ONCE

The first scenario involves selling your entire position at a target price. The problem with pegging your decision to sell your entire position at a single price is if the market does not fully achieve the price you are aiming to sell at.

Maybe you are targeting fifty dollars and you purchased at thirty. What if the market hits forty-nine dollars and then turns around for an indefinite amount of time? As a result of your all-or-nothing strategy, you missed out on profitability that could have been locked in if you were willing to sell a portion of your position incrementally. On the flip side, if the price does reach the target sell price as per your strategy, you maximize your possible return compared to other strategies.

This is the difficulty of exiting. **You make a trade-off between the probability of reaching the target sell point (circle 5) with the probability of maximizing return.** Simply put, the probability the price increases by 5 percent is greater than the probability the price increases by 10 percent. This is because in order to increase by 10 percent you must increase by 5 percent along the path to the 10 percent increase.

To briefly describe this with statistical terminology, the more standard deviations from the expected price (the EMPP), the less likely it is to occur under a short time frame. For example, a cryptocurrency worth one dollar is much more likely to reach ten and drop back down to five in under a month than it is to skyrocket to one hundred and return back to five. This isn't to say that in the long run the cryptocurrency isn't valued to be worth one hundred dollars using a quantitative model. Instead, understand that strategically, if you are looking to exit, sell targets closer to the current price target, which is more likely to occur than prices farther away.

QUICKLY

The second simple strategy you can use is to scale out quickly. This would involve selling more of your position at sell prices closer to the current price than your target quantitative sell price (circle 5).

Exit Quickly				
	Zone 2	Zone 3	Zone 4	Quantitative Model Target Price
% of Position sold	50%	20%	20%	10%

Figure 25: Exit Quickly

How do you decide how these sell zones are spaced? I would recommend having them placed at prices that are one-fourth of your target return that would be achieved if the target quantitative price is reached (circle 5). To simplify, if your target price is one hundred dollars and you purchased a crypto asset at fifty, you would achieve a 100 percent return if you sold at one hundred, doubling your position's value. Therefore, your zone increments would be at sixty dollars (20 percent return on original investment), seventy (40 percent return), eighty (60 percent), and ninety (80 percent). This leaves your original target price at one hundred dollars (100 percent return).

This is the most conservative exit strategy and aims to lock in as much of the profitability as soon as possible. The trade-off, as mentioned before, is less overall return than if the price continues to climb past the first and second sell zones all the way to the quantitative model target price (circle 5). On the flip side, if the market retraces before reaching the final sell increment, you have safely locked in profits, and still have a portion of your position to play with, as well as the potential to reenter and purchase more shares of the cryptocurrency than you originally had.

SLOWLY

The third strategy involves scaling out slowly. This involves selling more of your position at sell zones further away from the current price. This is the inverse of exiting quickly and aims to obtain a greater return by waiting longer to sell large portions of the position as the price rises—incurring greater risk (less likely to achieve this higher return).

Exit Slowly				
	Zone 2	Zone 3	Zone 4	Quantitative Model Target Price
% of Position sold	10%	20%	20%	50%

Figure 26: Exit Slowly

Note that you can have as many sell increments as you want. The problem is the more sell zones you execute at, the greater the total trading fees incurred because more trades are being executed. This cuts into the bottom line and reduces overall return. You can play around with how you scale out of a position and find what matches your risk profile.

PLANNING

Selling at a loss was discussed earlier in this work, but it is worth mentioning again briefly. **You must have preplanned exit prices (also known as "stop-losses") or zones for portions of your position.**[256] Most people view selling at a loss as failure when the reality is that selling is an opportunity to rebuy in at a lower price—expanding your number of shares or tokens and thus your potential profitability.

Preplanned exit zones should be placed anywhere from 6 to 30 percent below your buy price based on your aptitude for risk. Because crypto is so volatile, having large portions of your position ready to be sold at prices between −1 percent to −10 percent from your original buy price can be counterproductive because of price

bouncing back quickly from these temporary dips. More flexibility on your exit plan ultimately resides in your risk profile. As long as you understand the impact of your exit strategy on your potential return, you should be in a reasonable place.

Let's put everything together into a simple narrative of what entering and exiting looks like.

You identify a mispriced cryptocurrency according to your quantitative model and wait for an excellent entry price using EMPP as a general indicator. Next, you purchase the first of many purchases that will be spaced out every month using dollar-cost averaging.

Next, set sell increments between the current price and the quantitative model target sell price by evenly spacing these position exit points based on the return they would provide. Based on your return strategy and risk aversion, you will decide how much of your position you will sell if these price zones are encountered in the future.

Have the discipline to wait for your sell increments to be hit. **All the investment advice about strategic conviction and discipline discussed in previous chapters comes into play in the vast desert of time where you wait to execute your strategy sell zone strategies.** Many investors run toward the mirage of the sneaky promise of an impulse decision that ignores their original plan. When they arrive at the dried-up investing watering hole, they realize it was all an avoidable bad dream. **Entry and exit success is not about being the smartest guy in the room. It's about having a plan while being the most disciplined, patient, and emotionally and cognitively balanced investor you can possibly be.**

"The desire for constant action irrespective of underlying conditions is responsible for many losses in Wall Street even among the professionals,

who feel that they must take home some money every day, as though they were working for regular wages."[257]

—JESSE LIVERMORE

Having an entry and exit plan is leaps and bounds better than an investor that purchases or sells impulsively. The typical investor does a marginal amount of research and decides to purchase a cryptocurrency right in the moment. They then examine the charts further and realize they entered at a high price point as they watch the price tank (EMPP and moving averages reduce the chance of this mistake, but no promises).

Eventually, the price skyrockets past its initial entry. Because this unfortunate type of investor doesn't have a sell price target, they unwisely hold the crypto asset through the peak of the price movement. Eventually, the price retracts. Sadly, the investor is left holding the same amount of the crypto asset they started with, wishing they had sold on the uptrend and locked in some profitability. The new investor then sells their cryptocurrency with disdain, blaming the asset class.

If you fail to plan, then you plan to fail.

But you know better.

You now have some of the skills to be able to navigate the murky waters of entry and exit. No promises and no guarantees exist. But you can do your best to have a plan and execute on it when the time comes.

---

249 InvestorsLive, "[Weekly Lesson] Why Timing Is the Most Important Factor in Trading," Investors Underground, February 11, 2020.

250 Elizabeth Stapel, "Mean, Median, Mode, and Range," Purplemath, accessed June 4, 2020.

251 "What Is SMA?—Simple Moving Average," Fidelity, 2009,

252 Goldfarb and David A Kirsch, “Economic Bubbles Are Irrational, but We Can Understand Them—Brent Goldfarb & David A Kirsch: Aeon Essays,” Aeon, June 4, 2020.

253 “Cryptocurrencies,” MarketWatch, accessed January 12, 2018.

254 “Community Network Data,” Coin Metrics, accessed June 4, 2020.

255 lbid.

256 Stocktwits, Inc, “The Importance of Setting a Stop Loss and What It Means to Traders and Investors,” Medium, The Stocktwits Blog, July 22, 2016.

257 Lefèvre Edwin, *Reminiscences of a Stock Operator* (Mineola: Ixia Press, 2018).

CHAPTER 13

TAXATION & REGULATION

If you are anything like me, your brain shuts off when you read the word regulation. Taxation? Snooze fest. No one wants to read about how your money is viewed, taxed, or watched. Yet understanding how the historical powers of the world view your investment is valuable. Their story is just as much tangled up with blockchain and cryptocurrency as anyone else.

Assets are typically tangible, companies are physically auditable, and the systems in place are accountable to some known entity. Enter the gray area that is digitized assets and contracts built in a decentralized manner hosted on blockchains.

Many first-time investors get caught up in the excitement of investing. Tax sometimes becomes an afterthought.

"I feel like I might have accidentally ruined my life because I didn't know about the taxes."[258] Meet Reddit user *thoway*, a Californian office assistant who was making a modest $47,000 a year. A group of friends recommend he invest in Bitcoin in early 2017, so thoway purchased eight Bitcoin for the price of $7,200 per Bitcoin. In the next couple of months, the price of Bitcoin skyrocketed to $15,000 per Bitcoin and thoway sold all of his position, netting $120,000 for the sale!

This was amazing. A 108 percent return on investment is breathtaking. Unfortunately, thoway immediately reinvested this USD into other cryptocurrencies. What thoway realized in hindsight was that he owed income tax worth $50,000 on the initial profitable

sale of his Bitcoin for $120,000. During the time thoway took to realize he owed income taxes, the value of his reinvested position into other cryptocurrencies dropped to $30,000. He no longer had the capital to pay off the income taxes due for the initial successful sale of Bitcoin.

Stories such as thoway's are saddening, but the simple truth must never be forgotten. The IRS or whatever country you exist within expects to be paid a portion of your investment, which is only fair. You benefit from society; thus, you should contribute to society as a taxpaying compliant citizen.

THE POWERS AT PLAY

We shall start with the main players: Who cares about you as an investor?[259]

- Securities and Exchange Commission (SEC)
- Commodities and Futures Trading Commission (CFTC)
- Federal Trade Commission (FTC)
- Department of the Treasury
- Internal Revenue Service (IRS)
- Financial Crimes Enforcement Network (FinCen)

Not surprisingly, where money moves and how it moves is a huge concern for sovereign nations. These departments are all focused on collecting the fair share of money for the state, enforcing regulation such that investors are protected, and ensuring the trust and validity of markets in the eyes of the public as well as other nations remains stable. The major step in recent history is the classification of some crypto assets as securities. When an asset or contract is considered a security, the ramifications involve the mandatory compliance of the respective sovereign state. For our purposes, we will be examining the United States.

What is a security? While the official US legal definition is 145 words, with multiple pages defining each significant word, we will choose to use a simplified and still applicable definition:

"A security is an investment contract where an investment of money is made in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."[260]

To understand the precedent for how the SEC defines securities, we must travel all the way back to a Floridian citrus farm in 1946, run by The Howey Company.[261] This farming company decided to lease half of the land under its ownership to several businessmen "attracted by the expectation of substantial profits." The enterprise consisted of the businessmen providing investment money while The Howey Company provided the farming and the land. The businessmen provided the "capital," and The Howey Company provided the "work and management of the land." The businessmen had an expectation of "return" from The Howey Company under a lease contract. Seems fair enough, right?

It was fair, but fraught with risk.

The Howey Company litigation became known officially as the SEC v. W. J. Howey Co., 328 U.S. 293 case. The court ruled The Howey Company was a security because of the design of the investment contract. This is where the courts created what would eventually be known as the infamous "Howey Test."[262] The test of whether a transaction, asset, or ambiguous stand-in is an "investment contract" (a security) under the Securities Act is whether the scheme involves an investment of money in a common enterprise with profits to come solely from the efforts of others. Anything that holds the label of "security" has an entire set of rules and regulations that must be followed in order to protect investors. It is expensive and is why being identified as a security is such a big deal.

If the "investment contract" test is satisfied, the next step of the Howey Test is concerned with if the contract is immaterial or material, speculative or nonspeculative, and whether a sale of property with or without intrinsic value goes on. That is to say, if a contract involves an investment in which you do nothing, with the expectation set in advance that a certain return will be given to you based purely on capital, then you have entered into the territory of said contract being classified as a security.

This is where things get tricky. **Currency is not a security.**[263] Currency is a medium of exchange, not a generator of return based on management by a third party. This sentiment was backed up by the SEC Chairman in 2018, who confirmed in a CNBC exclusive interview that cryptocurrencies such as Bitcoin are not securities.[264] This is because cryptocurrencies have the properties of a currency and do not contractually promise a certain return, in contrast to a traditionally defined security. In addition, while the "speculative" portion of the Howey Test is satisfied, because blockchain is decentralized, **no managerial efforts of a single party can be pointed to by the SEC or any regulatory body.** This is unprecedented. It's a deep space wormhole that pulls investor money in, without the possibility of reaching the center of it all, because there is no centrality. No single party.

Caution is still due. **No official statement concerning Bitcoin as a security has been released by the SEC (an interview does not count as an official statement).** This by and large remains one of the greatest risks many cryptocurrencies face—regulations and the impact of the law on investors who own Bitcoin could be heavy.

SEC CLAMPS DOWN

Has the SEC given up its ability to go after cryptocurrencies? Absolutely not.

Enigma began in 2015 at the MIT Media Lab. It started off as a humble white paper focused on creating the privacy layer for the decentralized web. Enigma raised $45 million during its ICO in return for "ENG," the cryptocurrency of the Enigma blockchain. As one of the oldest projects, it was one of the first blockchain protocols to lead the charge. The team touted a long-term vision, regular development updates, and a soon-to-be-live testnet. Enigma MPC was based in San Francisco and Israel, with team members from all over the globe.

On February 19, 2020, the SEC announced it settled charges against blockchain technology startup "Enigma MPC" for conducting an unregistered offering of securities.[265] Enigma agreed to return funds to harmed investors via a claims process, register ENG digital tokens as securities, and file periodic reports with the SEC. Finally, Enigma MPC paid a hefty charge of $500,000. Remember when risks were discussed earlier? This is a perfect manifestation of a risk that was qualitatively predictable.

While the SEC didn't outline the exact reasons for why ENG was classified as a security while Bitcoin was not, it boils down to a very basic concept.[266] When investors purchased the digital asset ENG, they had an expectation that the **management of the protocol by Enigma MPC would yield a certain amount of return**. Because the protocol was **not decentralized in its ownership and design**, the agency of the protocol was firmly attached to Enigma MPC the company. Combine that with speculation and an immaterial contract, and suddenly you've passed the Howey Test. **This is not so for other blockchain protocols** that are **decentralized** by design with decentralized control of the protocol such that **no single party** has the burden of needing to provide a certain return.

Hope for a blockchain protocol such as Enigma exists, but litigation is a huge setback. Enigma is now establishing a new truly decentralized network not controlled by Enigma MPC. The token on the network is called SCRT (Secret Token) and will not be classified as a security by the SEC because the network is properly decentralized and therefore falls into the same unclassified/decentralized category as Bitcoin.[267] Enigma may see a future in which its protocol is widely developed, extended, and used by hundreds of different use cases. For now, the future remains shrouded in risk.

What are the ramifications of this type of event? Investors lose trust, developers move to sustainable platforms, and price drops off a cliff. In Enigma's case, **ENG lost 80 percent of its value in just under 30 days after the SEC announcement**, a humble reminder of the volatility and unknowns of the Wild West that is cryptocurrency. This is the power of the SEC on display—not all projects will have the liquidity and capital to survive a long-standing litigation with the SEC.

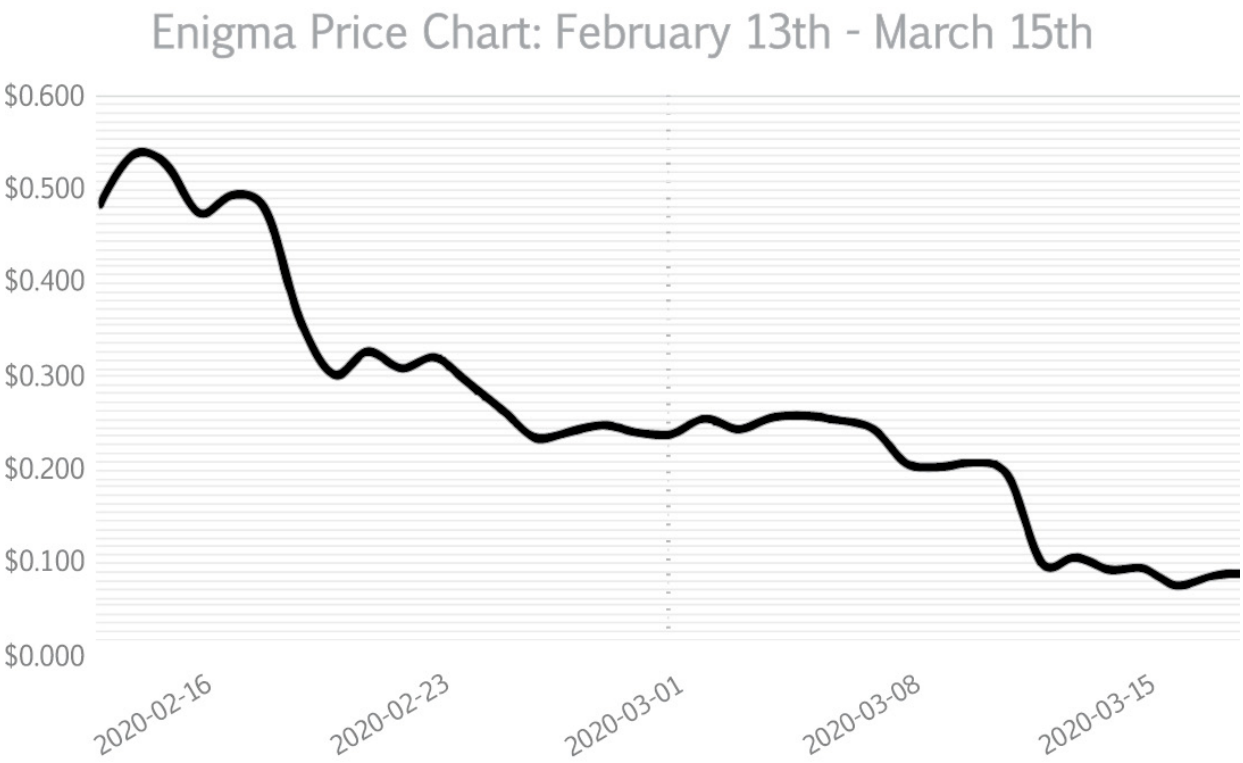


Figure 27: Enigma SEC Price Drop

Enigma was not the first ICO-turned-SEC litigation, nor will it be the last. While protection of the consumer is cited on many occasions, the truth is that a lot is at stake. Anything that would threaten the hegemony of the United States and the power of the dollar as the de facto global currency is immediately under intense suspicion. Congressmen have on multiple occasions called for a complete ban on cryptocurrencies under this very basis. Donald Trump has openly stated on Twitter, "I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air."[268] He has also stated there is only one real currency in the United States, the United States Dollar. This is ironic considering a survey by HSB revealed 36 percent of small to medium businesses in the US accept Bitcoin.[269] Major companies that accept Bitcoin are AT&T, Expedia, Microsoft, and everyone's favorite data silo, Wikipedia.[270] Clearly bankers are concerned, and you can't blame them. **Decentralized technology is the exact antithesis of**

those who believe in the central control of technology and monetary policy.

"An awful lot of our international power comes from the fact that the US dollar is the standard unit of international finance and transactions. Clearing through the New York Fed is critical for major oil and other transactions. It is the announced purpose of the supporters of cryptocurrency to take that power away from us, to put us in a position where the most significant sanctions we have against Iran, for example, would become irrelevant."[271]

—CONGRESSMAN BRAD SHERMAN

Fear not, one representative's negative view of cryptocurrency is not universally accepted. Utah has put favorable regulations in place to help encourage blockchain innovation within their own borders. The "Blockchain Technology Act" (Bill 0213) excludes blockchain businesses from money transmitter compliance standards—a problem that is stifling innovation in other states.[272] Other states have also begun toying around with state legislation outlining rules specifically for cryptocurrency and blockchain technology.[273] Andrew Yang, a 2020 presidential candidate, is known for wanting to bring clarity in the regulatory space from a federal standpoint.

"Right now we're stuck with this hodgepodge of state-by-state treatments and it's bad for everybody: it's bad for innovators who want to invest in this space. So that would be my priority is clear and transparent rules so that everyone knows where they can head in the future and that we can maintain competitiveness."[274]

—ANDREW YANG

CLASSIFICATION

The Crypto-Currency Act of 2020 proposed by Arizona Congressman Paul Gosar aims to classify crypto assets. This regulatory clarity is one of the first comprehensive pieces to be written up in the United States and will more than likely be a guiding piece of legislation for future proposals.[275] Important regulatory oversights were the classification of cryptocurrency into three different categories.[276] This is where language is beginning to evolve in the regulatory space. While this book took a broad swing at pinning down legislative intent as it pertains to semantics, language will continue to evolve as regulatory frameworks are established to classify and regulate the various crypto asset classifications.

- Crypto-commodities—regulated solely by The Commodity Futures Trading Commission
- Crypto-currencies—regulated by FinCen and the Treasury
- Crypto-securities—regulated solely by the SEC (discussed earlier in this chapter)

Crypto-commodities (as defined by this bill) are economic goods or services that have full or substantial fungibility, rest on a blockchain or decentralized cryptographic ledger, and are treated by the market with no regard to who produced the good or service. **In what way is a commodity different from a currency?** A commodity is an object with use value and can be exchanged. A commodity also can experience a deviation in price based on market expectation of future supply and demand. Grain, precious metals, electricity, oil, and beef are all classical examples of commodities.

Take electricity as an example: electricity is used for commercial, residential, industrial, and transportation purposes. Electricity's value fluctuates based on how much electricity is demanded and supplied on any given day.[277] After a hurricane, many different oil and gas refineries (located along the Gulf Coast between Houston and

Louisiana as an example) are negatively impacted. When operations shut down for repairs post storm, less supply is available, increasing the price of electricity. Generally, we don't care where the electricity comes from, as long as our phone is able to be charged, the lights turn on, and the computer boots up. Because electricity can be traded, exchanged, speculated on, and used, we are able to confidently define it as a commodity and regulate it as such.

But wait a moment, isn't Bitcoin a cryptocurrency? Isn't that the assumption we have run under?

Doesn't Bitcoin sound a lot like a crypto-commodity? First, let's return to the bill's definition of a crypto-currency.

A **crypto-currency** in this proposed bill is defined as:

"Representations of United States currency or synthetic derivatives resting on a blockchain or decentralized cryptographic ledger. Such representations are reserve-backed digital assets that are ***fully collateralized in a correspondent banking account such as stablecoins.*** *Synthetic derivatives are determined by decentralized oracles or smart contracts and are collateralized by crypto-commodities, crpyto-currencies, or crypto-securities."*[278]

Facebook's Libra was shoved into national attention in 2019 and is an example of a crypto-currency by this legislation's definition.[279] Libra was a "stablecoin" designed to be a one-to-one equivalent with the US dollar, backed by Facebook's bank account. This is what makes a stablecoin; a digital asset that is guaranteed to be a one to one equivalent with another currency.

Why did Facebook want to create this currency?[280] According to Mark Zuckerberg, Libra would make sending money "as simple as sending photos." You would quite literally be able to "text" currency in terms of functionality. In addition, over 1.7 billion adults without bank

accounts (but with access to Facebook) would be able to use Libra as a means of exchange. The Libra Association is a consortium of companies aiming to launch a cryptocurrency shared on multiple different platforms.[281] While Facebook is technically not the direct owner of the to-be Libra blockchain, Facebook has a significant amount of clout in decision-making.

In the end, legislators attacked Libra as an attempt to usurp US dollar dominance. Seven of the original twenty-eight founding members dropped out before the Libra Association's inaugural meeting in Geneva on October 14, 2019. These members that dropped out included PayPal, eBay, Stripe, Visa, and MasterCard.[282] Essentially, the industry giants got cold feet. You can't blame them, either**—no centralized group of entities wants to go toe-to-toe with the full force of the US regulatory system.** It is not to be messed with.

Cryptocurrency is the universally accepted term (as of now) for a digital token that holds and represents value—hosted on the blockchain and exchangeable between mutually distrustful parties. While this piece of literature used this as the working definition, regulators are heading in a direction where, for all intents and purposes, the cryptocurrencies that you can invest in and see a return on are considered to be either a crypto-commodity (Bitcoin) or a crypto-security by the regulatory space.

Now that we have a better understanding of the classification of cryptocurrency, how does regulation manifest itself with your dollars? It comes forth in the form of a power as old and strong as death itself.

"In this world nothing can be said to be certain, except death and taxes."

—BENJAMIN FRANKLIN

TAXATION

Taxes. Love them or hate them, the civilization you exist within depends on the fair contribution of citizens paying back into the sovereign nation in order to maintain the public good—to create a stable society enabled by the unspoken agreement we all play by. This is made possible by your labor in tandem with the collective whole of society. You are legally obliged to follow the law to the best of your ability. The walk-through I have given and will proceed with should always be triple checked. This is not financial advice; all financial decision-making is your own. Taxation and the law are ever changing. **Always be weary of what you read from the past and always fact-check with the most current reality.**

Disclaimer: This section is informational and should not be construed as a placeholder for tax or investment advice. Please speak to your own CPA, tax attorney, or tax expert on how you should treat taxation of digital currencies and digital assets.

As of the tax laws valid for January 1, 2020, cryptocurrencies of all ambiguous forms are considered property as it pertains to taxes. Because of this, you are subject to the rules surrounding capital gains and capital losses.

What is a capital gain? It is the rise of value of a capital asset (property-like assets) that gives it a higher worth than the purchase price.[283] If I purchase an asset for $100 and then turn around and sell it for $200, I have just made a capital gain. The inverse is true for a capital loss.[284]

What is a taxable event for crypto-commodities and crypto-securities? Is it if I purchase coffee with Bitcoin? What if I gift a

friend Ethereum or buy some cryptocurrency from an exchange?

Fortunately, the IRS took action in 2014 and outlined **precisely** what the rules are in a six-page document titled **"Notice 2104-21."**[285] I would encourage you to look this up and read from the horse's mouth. Despite the fact that definitions from a regulatory perspective are consistently shifting, we can confidently follow the following rules as of the time this book was published.

A taxable event for crypto (for which tax reporting is a requirement) are the following:[286]

- Earning crypto as income
- Using crypto for goods and services
- Trading crypto for a different crypto
- Trading crypto to fiat currency (such as the US dollar)

A taxable event for crypto does **not** include the following:

- Buying crypto with USD
- A transfer from one digital wallet to another
- Giving crypto as a gift—a transfer of property for less than its full value (as defined by the IRS)[287]

People are fighting for the ability to purchase items with cryptocurrency without triggering a capital loss or capital gain. I fully believe that in the future, as stablecoins are adopted in their many hybrid forms, legislation will reflect this needed change.

You must have a record of all your taxable events, as you need to submit an IRS form 8949 as well as a 1040 Schedule D on a yearly basis.[288] Services such as TurboTax help with the submission of the form, but you need to be able to provide the inputs. If you are wondering the exact mechanics of recording a taxable crypto event, plenty of online videos that are up to date can walk you through the

series of steps. It would be worth starting a spreadsheet containing a consistently updated log of the following required 8949 entries:

- The amount of property (such as five Bitcoin)
- Cost basis in USD (what rate you bought the crypto for, including fees)
- The date of purchase
- Fair market value in USD (what rate you sold the crypto for, as well as the amount sold)
- The date of sale
- Gains and losses in USD

At the end of the tax year you will summate all your taxable events, resulting in either a net positive or negative situation. Your investment log is an objective view into your crypto investments, and as a side effect can simultaneously be the basis for tracking the entries that are the basis for filling your 8949 and 1040.

After your overall capital gains or losses have been determined at the end of the year, How is the rate the capital gains are taxed determined? In layman's terms, *"What is the tax rate on my overall profit (or loss)?"* **It depends on if either short-term capital gains or long-term capital gains apply to you, as well as your income bracket.** Short-term capital gains are if the sale of the property (in this case crypto) has been less than or greater than twelve months since the original purchase. If the sale is under twelve months from the original purchase, short-term capital gains apply. If the sale is over twelve months from the original purchase, long-term capital gains apply. Listed below is the 2020 tax brackets in the United States.

Table 1.2020 Tax Brackets and Rates

Rate	For Single Individuals, Taxable Income Over	For Married Individuals Filing Joint Returns, Taxable Income Over	For Heads of Households, Taxable Income Over
10%	$0	$0	$0
12%	$9 , 875	$19, 750	$14, 100
22%	$40 , 125	$80, 250	$53, 700
24%	$85 , 525	$171, 050	$85, 500
32%	$163 , 300	$326, 600	$163, 300
35%	$207 , 350	$414, 700	$207, 350
37%	$518 , 400	$622, 050	$518, 400

Source: Internal Revenue Service

Figure 28: Short Term Capital Gains[289]

This is in stark contrast to an individual who sells a crypto asset after the twelve-month period. Long-term tax rates are significantly lower and reward individuals who have patience and conviction about their investment. This is why picking your time horizon as mentioned earlier in the book is so important. It can be the difference between a small gain and a large gain because of capital gains tax. Listed below are the long-term capital gains brackets for 2020.

Table 6. 2020 Capital Gains Brackets

Rate	For Single Individuals, Taxable Capital Gains Over	For Married Individuals Filing Joint, Returns, Taxable Capital Gains Over	For Heads of Households, Taxable Capital Gains Over
0%	$0	$0	$0
15%	$40, 000	$80, 000	$53, 600
20%	$441, 450	$496, 600	$469, 050

Source: Internal Revenue Service

Figure 29: Long Term Capital Gains[290]

Because of the perceived lack of regulation from the SEC and other regulatory bodies, some investors have taken it upon themselves to not pay taxes, not record their transactions, and to not follow the

law. In order to onboard your fiat into cryptocurrency, you need to go through an exchange that transacts with banks. Those exchanges are compliant with the US authorities, and therefore are held responsible by Know Your Customer standards. Right off the bat, you are "in the system" when you send your cryptocurrency to a different wallet from your exchange wallet. **Your real-world identity could conceivably get attached to that digital wallet**.

Because the majority of large public blockchains are entirely transparent, the chain of transactions from the wallet receiving the funds (from the exchange) to any other wallets is visible. By design, public blockchains are accessible to everyone in the world—anyone can see the entire set of transactions on a blockchain all the way back to the very first transaction. This is what makes a blockchain immutable and auditable.

This is to say that even if you are transacting with decentralized exchanges or smart contracts separate from an exchange, you are not immune or invisible from the government. Your public wallet address may be 0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2 and completely "anonymous" to 99 percent of the individuals using the blockchain, but if an exchange has somehow attached your Know Your Customer exchange identity to this wallet, then you are no longer outside of the system.

You are responsible for your financial transactions.

"Mixers" are considered some of the most dangerous technologies by regulators.[291] Mixers aim to obfuscate transactions by having groups of wallets swap hundreds of different denominated amounts between wallets, making it difficult to track a sender and receiver. The funds will eventually reach their intended target but will arrive at the wallet from multiple different wallets, confusing any sort of tracking algorithm trying to detect which wallet was the original sender and

even who was the intended receiver. This is an arms race of technology, and you can count on the fact that the IRS or FinCen have some of their best software engineers designing programs to track wallets through these various obfuscation services.

At the end of the day, you must do your due diligence. Track your transactions to improve yourself as an investor and to also pay your taxes properly. Always be on the lookout for legislation and regulation that will impact your investment vehicle. Be aware of the risks of not properly following the law, even unintentionally. As John Marshall, a lawyer and politician from the early 1800s, stated, *"The power to tax is the power to destroy."*

Don't end up on the wrong side of the fence.

---

258 thoway, "r/Personalfinance—I Just Discovered That I Owe the IRS $50k That I Don't Have, Because I Traded in Cryptos. Am I f*****?," reddit, accessed June 4, 2020.

259 "International Legal Business Solutions—Global Legal Insights," GLI—Global Legal InsightsInternational legal business solutions (Global Legal Group), accessed December 17, 2019.

260 "15 U.S. Code § 77b—Definitions; Promotion of Efficiency, Competition, and Capital Formation," Legal Information Institute (Legal Information Institute), accessed February 7, 2020.

261 BitTrust, "Passing the Howey Test: How to Regulate Blockchain Tokens," Medium, (BitTrust, March 4, 2017).

262 "SEC v. Howey Co., 328 U.S. 293 (1946)," Justia Law, accessed June 4, 2020.

263 Kate Kooney, "SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies," *CNBC*, June 11, 2018.

264 lbid.

265 Nikhilesh De, "ICO Project Enigma Settles SEC Charges Over $45M Token Sale," CoinDesk (CoinDesk, February 19, 2020).

266 "Press Release," SEC Emblem, February 19, 2020.

267 Enigma Project, "Introducing Secret Network," Medium (Enigma, May 27, 2020).

268 Donald J. Trump, "I Am Not a Fan of Bitcoin and Other Cryptocurrencies, Which Are Not Money, and Whose Value Is Highly Volatile and Based on Thin Air. Unregulated Crypto Assets Can Facilitate Unlawful Behavior, Including Drug Trade and Other Illegal Activity . . . .," Twitter, July 12, 2019.

269 "HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency," Business Wire, January 15, 2020.

270 Matt Anderson et al., "Who Accepts Bitcoins in 2020? List of 20+ Major Companies," 99 Bitcoins, accessed June 4, 2020.

271 Coin Center, "Today in Congress Rep. Sherman Called for a Bill to Ban All Cryptocurrencies," Twitter, May 9, 2019.

272 Christine Gilbert, "Blockchain Technology Act," SB0213, May 14, 2019.

273 Carlton Fields, "State Regulations on Virtual Currency and Blockchain Technologies—(Updated)," JD Supra, April 19, 2019.

274 "US Presidential Candidate Andrew Yang Says Regulations Cannot Impede Crypto," Bitcoin News, February 1, 2020.

275 "What Is the Cryptocurrency Act 2020?," Yahoo! Finance, January 7, 2020.

276 Paul Gosar, "Text—H.R.6154—116th Congress (2019-2020): Crypto-Currency Act of 2020," Congress.gov, March 9, 2020.

277 Lawrence Pines, "Electricity: Learn How To Trade It at Commodity.com," Commodity.com, August 16, 2019.

278 Paul Gosar, "Text—H.R.6154—116th Congress (2019-2020): Crypto-Currency Act of 2020," Congress.gov, March 9, 2020.

279 Robert Kim, "Analysis: A Crypto-Currency Act of 2020? You Cannot Be Serious!," Bloomberg BNA News, January 13, 2020.

280 Andrew Morse, "What You Need to Know about Facebook's Libra Cryptocurrency," CNET, October 24, 2019.

281 Josh Constine, "Facebook Announces Libra Cryptocurrency: All You Need to Know," TechCrunch, June 18, 2019.

282 Josh Costine, "Facebook Crypto Consortium Libra Association Has Lost 8 'Founding Members'," Yahoo! Finance, October 11, 2019.

283 James Chen, "Capital Gain," Investopedia, January 29, 2020.

284 Ibid.

285 IRS, "Notice 2014-21," April 14, 2014.

286 David Kemmerer, “The 2020 Guide To Cryptocurrency Taxes,” RSS, January 2020.

287 “Gift Tax,” Internal Revenue Service, accessed June 4, 2020.

288 CryptoTrader Tax, “Crypto & Bitcoin Taxes Explained—Everything You Need To Know | CryptoTrader.Tax,” July 31, 2019, Video, 11:56.

289 Amir El-Sibaie, “2020 Tax Brackets,” Tax Foundation, March 13, 2020.

290 lbid.

291 Osato Avan-Nomayo, “Cryptocurrency Mixers and Why Governments May Want to Shut Them Down,” Cointelegraph (Cointelegraph, May 28, 2019).

CHAPTER 14

INVESTING WITHIN YOURSELF

"Money is just something you need in case you do not die tomorrow. Let this be a reminder for you not to obsess over profits and losses. In whatever you do, strive for enjoyment, focus, contentment, humility, openness."[292]

—Yvan Byeajee

It has been a journey.

As an investor and learner, you will always have ups and downs, but how you choose to throw yourself into the learning curve, the struggles, and the storm is what makes you wiser. If I wish I would have known a couple things sooner, they would have been this: **Embrace change quickly**. With technology evolving as fast as it is, the world is wide open to those who take the leap of faith into trying to understand, explain, and invest into emerging technologies.

When I talk about taking a "leap of faith," what does it look like?

From all the individuals I interacted with in the investing and computer science domain, I can confidently say your work ethic, your attitude toward failure, and your habits are what define your ability to learn new information and then synthesize it into actionable steps.

This book aims to teach you what it means to take actionable steps to investing in cryptocurrency. It equips you with all the tools necessary to examine a cryptocurrency with qualitative analysis and even some with basic quantitative models. Your quantitative and qualitative skills are what separate you from the pack.

"Power is defined as an ability to do qualitative work with a quantitative passion, backed by a

compelling conviction, directed by a propelling purpose, fulfilling a divine destiny."[293]

—ISRAELMORE AYIVOR

You now know how to plan your entries and your exits in advance and what it means to have a diversified portfolio. You now have a solid understanding of how blockchain works as well as what properties make it valuable. In addition, you also know how blockchain fits into the big picture, even in context of regulatory entities such as the US Federal Reserve and the IRS.

Human nature is limiting—we've explored stories of what happens to those who become greedy or fall prey to a range of cognitive biases and weaknesses. From Rob P. Gekwiak's story of rags to riches and then back to rags again, all the way to Simon Golestan and his $337,000 portfolio dropping to $20,000. We've examined the story of cryptocurrency in Zimbabwe and how regulatory giants in the US are attempting to take down targets that are not decentralized enough (such as Enigma).

At the start of this book I introduced the "Skepticism Factors": Volatility, Trust, and Tangibility. These are the barriers of entry for institutional investors, and for everyday people like you and me. As adoption increases and the technology improves, the skepticism factors will disappear as cryptocurrency begins to be perceived as having intrinsic value.

After inspecting volatility, you should now know it stems from a range of qualitative risks such as project complexity and liquidity. This does not make cryptocurrency a bad investment, it simply adjusts our expected return and gives us a foundational

understanding of how much risk is involved with investing in the wild west of asset classes.

When it comes to trust, we've explored the exciting use cases of blockchain solving mistrust between mutually distrustful parties—from identity management, health care, and all the way to financial instruments.

Smart contracts are the wave of the future, replacing human third parties with the equivalent of digital vending machines. Every industry will be affected by this, and it's a race to see who can incorporate and build the best possible blockchain that will have the greatest amount of adoption. We know blockchain creates trust, and we now understand what "trustless trust" means (immutable, censorship resistant transactions and smart contracts anyone can interact with). Soon, we will trust mathematics and immutable open-sourced code to be the facilitator of our peer-to-peer transactions, not centralized data silos and human third parties such as Facebook and PayPal.

Yet in order to make cryptocurrency feel tangible, you have to go out into the "wild" and play with it. That is the final step. Until you are sending Bitcoin to your brother to pay him back for Starbucks, you won't quite be at the stage where crypto feels tangible. Now that you understand the gears and levers of blockchain, I would encourage you to purchase a small amount of cryptocurrency and begin to play around with a crypto wallet and its many possible interactions with thousands of decentralized apps.

If you want the tangible steps to purchase cryptocurrency, move it around, and interact with decentralized apps, you can go to "CarterLWoetzel GitHub," where you can click on "Building Confidence in Blockchain—Next Steps."[294] There, I have also

provided links to other helpful blockchain learning resources as well as my own quantitative models for you to play around with. The time for you to put the book down and actually take action is almost here, but first let me conclude our time together.

Together we have unraveled the tangled web of blockchain and mapped a more accurate and realistic view of the complicated and often misunderstood asset class that is cryptocurrency. You are now an empowered investor ready to tackle cryptocurrency as an asset class. However, the most valuable lessons you will learn about investing in cryptocurrency can only come from jumping into the deep end. **Make mistakes and take informed risks but attempt to do it the right way.**

You now have a fifty-thousand-foot view of the "magic of blockchain," so when your coworker or friends ask, "How does this whole blockchain thing work? What is cryptocurrency and why should I care?" you can pause, smile, and then **confidently** say, "It's complicated . . . but if you give me five minutes of your time, I can try to explain. . . ."

And that, my friends, is a beautiful thing.

—Carter Lee Woetzel

---

292 MWCM, "Principles of Success Part II: 'Don't Chase the Money'," MW Capital Management Pte Ltd., October 19, 2018.

293 Israelmore Ayivor, *Michelangelo / Beethoven / Shakespeare: 15 Things Common to Great Achievers*, 2013.

294 Carter Lee Woetzel, "CarterLWoetzel/Building-Confidence-in-Blockchain---Next-Steps," GitHub, June 6, 2020.

ACKNOWLEDGMENTS

Writing a book on investing in an emerging technology was an opportunity of a lifetime. I have been inspired and supported by so many along the way. Here are the individuals that have made this story and three-year journey possible by contributing to the presale campaign.

Todd Trosclair—a friend and true supporter of those who dream big.

Chris Postiglione—a writer at heart; the first five syllables of my haiku.

Jay Barnes—for your impact on my college education.

Ross Allen—thank you for your leadership amid these trying times.

Connor Schmidt—the first to purchase a book. A dear friend I have shared many laughs with.

Matthew Eng—for your ferocious passion for learning.

Logan Jacobsen—one of the hardest workers I have ever met.

Rachael Bausman—for inspiring so many students to go above and beyond, to dream big.

Eric Koester—for helping many to become first time writers as if it was our second book.

John Beacham—amidst a crazy 2019–2020, you centered me on what truly matters. Thank you for your mentorship.

Grant Woetzel—because comedians are often the smartest people in the room.

Garrett Woetzel—you took the time to message me some links on LinkedIn; Who would have thought that would lead me to where I am today three years later?

Mara Short—Marzy, your authenticity brings joy to so many, including me.

Carl Woetzel—your willingness to share your business stories give such excellent insight consistently.

Craig Woetzel—a warm and playful soul who makes everyone feel seen.

Jordan Patros—for listening to someone passionate about blockchain.

River Beard—Lissner lobby, never forget!

Jacob Stand—a straight shooter if there ever was one. I appreciate your honesty and hard work.

Clint Carney—a world changer, undoubtedly. You live life to the fullest, and it makes me want to as well.

Babu Wanyeki—my first friend in high school, thank you for continuing the journey of learning.

Bryn Loftness—some people say they will change the world, others go do it. Excited to see you continue to climb.

Drew Johnson—the hardest working team member I have ever seen.

Whitney Brown—for supporting a first-time author.

Josiah Huffman—a friend no matter how much time passes.

Vinayak Rajesh—for pushing me to think deeper, solve better, and run harder.

Matt Barton—your love of mathematics rubbed off on me somehow. I consider it a miracle.

Jordan Nimlos—an ethical, kind, and inspiring colleague. I will never forget the HD summer!

Dakota Holman—thank you for putting up with all my sleepless nights and blockchain jabber!

Austin Woetzel—your support and character have never gone unnoticed. Love you brother.

Maria Woetzel—for being my biggest fan, through my crazy highs and lows.

Grandpa & Grandma Osborn—words will always fail to describe what you have done for us kids through your many sacrifices. God bless.

Jonathan Michelson—for letting me pull you into cryptocurrency, for better or for worse!

Jonathan Sweeney—the best captain there ever was.

Andrew Hintz—because I can dance like a maniac with you, and you don't question it.

August Postiglione—family is forever. Thank you for all the memories we have made.

Justine Evenhouse—for surviving managerial accounting with me and promoting the book.

Marianne Stephen—for supporting all the way from Pennsylvania!

Clay Anderson—for supporting a fellow student.

Ann van Heerden—your passion for learning is infectious and has had a deep impact on me.

Tyler Bethke—Trials of miles, miles of trials.

Tony Harris—because settling is boring, and action is everything.

Karl Olsen—raw work ethic and inclusiveness, I aspire to be more like you.

Cody Holz—because B2 is forever.

Anja Wiita—for putting up with me in Operations Research.

Joyce LeMay—for teaching the power of management.

Tammy Holman—for your love of nature.

Drew Whitson—your teaching at Bethel has and will continue to impact countless students' careers, mine included.

Alec Sonquist—but you have heard of me . . . (hint, your favorite movie).

John McCauley—for walking the straight and narrow.

Jacob Stein—because you bring truth and authenticity.

Jeremy Schipper—for calling me out on my BS, consistently.

Jeremiah Zilka—a fellow morose soul that knows how to have fun despite the many ups and downs of life.

Karsten Skoglund-Anderson—for making me look at art and film deeper than I had before meeting you.

Thomas Saatzer—because self-defense, personal growth, and laughter can all go hand in hand.

Katie Sibbet—a family friend and a courageous pursuer of equity and truth.

Marcus Cundiff—a fellow Blaine alum who chose to support the book despite having not seen me in years.

Pat Osborn—you have a witty charisma I can only hope to channel even slightly in a book such as this.

Emily Klassen—the hardest I have ever laughed with someone because of our hopeless attempt to make some semi-accurate Excel models.

Alex Hintz—for continuing to support the inescapable Woetzel-Hintz legacy.

Curt & Kelly Woetzel—whom I love dearly. And always will.

Zachary Nelson—for having such a strong impact on the Bethel Investment Fund.

Linda Goodwin—because of your incalculable impact through Bethel's mentorship program.

Raj Vinjamuri—because you never know when you will cross paths with a fellow innovator.

Brian Jemming—for your fortitude and friendship with the Woetzel family.

Theodore Krumholz—true respect for your finance and investing skill, aptitude, and leadership.

Elizabeth Vang—because pursuing what is meaningful impacts those around you unwittingly.

Alex Becker—never is there a boring day if you show up.

Frances Piper—you have an intense curiosity and empathy I appreciate deeply.

Chessa and Anthony Miller—because of your countless visits with games and cake that fueled this book.

Annamarie van Heerden—for convincing me that maybe . . . just maybe . . . Texas is in fact a better state than Minnesota.

Calvin Friedrich—for continually showing me the power of practical skills and how I lack them immensely.

Matthew Bunker—because some suffering only fellow computer scientists can understand.

Joshua Klukas—your deep thinking and love of running continues to influence me to this day.

Meckenna Woetzel—A future author, mark my words.

Zack Skubic—from the Blockchain education network—I will follow up as soon as this is published!

Seth Gunderson—an adopter of emerging technology and ideas far quicker than the average person.

Patrice Conrath—for teaching me what it means to lead with grace by faith.

Jayde Blackburn—for all the laughter you have created inside of the Happy-Lab!

Deborah Thomas—for giving me the building blocks that made this whole thing possible.

Nathan Gossett—for showing me how little I know, and how much further I have to go.

Bruce Olsen—for teaching me how to read a balance sheet and laugh while doing it.

Holly Boisjolie—for pestering me to join BPA. You were the beginning of so many stories and journeys because you had confidence in me as a person and as a student.

Gretchen Kulas—for teaching me physics, which would lead me (somehow) to obtain a mathematics minor.

Mr. Fedor—because I will never forget the education Blaine High School provided—you invest in students as people first. God bless.

A special thank you to my editor Nick Mancuso—laughter makes for better writing. Also thanks to Tor Bair of the Secret Foundation for your many insights on blockchain the last couple of years. Finally, thank you to Ryan Porter. Your honesty and drive to make this book lean and mean helped create a far better book than I ever could have imagined.

APPENDIX

INTRODUCTION—BLOCKCHAIN AND TRUST

•AlgoShare. "To Centralize Is Human, to Decentralize Divine." Last Modified November 20th, 2018. https://medium.com/@AlgoShare/to-centralize-is-human-to-decentralize-divine-1353247113bd.

•Bair, Tor. "The True Enemy of Decentralization." Last Modified February 26th, 2018. https://medium.com/@TorBair/the-true-enemy-of-decentralization-500065a26fb5.

•Chaum, David. "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." (PhD dissertation, University of California—Berkeley, 1979). 1-40. https://www.chaum.com/publications/research_chaum_2.pdf.

•Clarke, Arthur C. Profiles of the Future: an Enquiry into the Limits of the Possible. London: Pan, 1983.

•Featherston, Ed. "Blockchain: You Want Me to Trust a 'Trustless Trust' System?" Last Modified November 15th, 2017. https://www.cloudtp.com/doppler/blockchain-you-want-me-to-trust-a-trustless-trust-system/.

•Fuller, C. R. "The Economic Foundations of Authoritarian Rule." (PhD dissertation, University of South Carolina, 2017) 169-171, https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=5219&context=etd.

•Fuller, C. R. "The Economic Foundations of Authoritarian Rule." (PhD dissertation, University of South Carolina., 2017) 1-14, https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=5219&context=etd.

•Green, Olya. "Re-Imagining Money: Are the 700 Years of Centralization over Now?" Hacker Noon, May 6, 2020. https://hackernoon.com/re-imagining-money-are-the-700-years-of-centralization-over-now-be97979d30f9.

•Mostazo, Lucas. "What Is Blockchain? the Best Explanation of Blockchain Technology." January 14th, 2018. Video, 6:26. https://www.youtube.com/watch?v=3xGLc-zz9cA.

•Nakamato, Satoshi. "Bitcoin Open Source Implementation of p2p Currency." Satoshi Nakamoto Institute. Last Modified February 15th, 2009. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/2/.

•Sims, David. "Hollywood Makes Way for the Disney-Fox Behemoth." The Atlantic, Atlantic Media Company. Last Modified March 21, 2019. www.theatlantic.com/entertainment/archive/2019/03/disney-fox-merger-and-future-hollywood/585481/.

•Sueur, Cédric, et al. "From Social Network (Centralized vs. Decentralized) to Collective Decision-Making (Unshared vs. Shared Consensus)." PLoS ONE, vol. 7, no. 2, 2012, doi:10.1371/journal.pone.0032566.

•Tabora, Vince. "The Evolution of the Internet, from Decentralized to Centralized." Hacker Noon, October 27, 2019. https://hackernoon.com/the-evolution-of-the-internet-from-decentralized-to-centralized-3e2fa65898f5.

•Thu, Kendall. "The Centralization of Food Systems and Political Power." Culture & Agriculture 31, no. 1. June 8, 2009. 13–18. https://doi.org/10.1111/j.1556-486x.2009.01013.x.

•"Why Decentralizing Social Media Makes Sense." Social Media Explorer. Nov.ember 20, 2018. https://socialmediaexplorer.com/social-media-marketing/why-decentralizing-social-media-makes-sense/.

CHAPTER 1: BLOCKCHAIN & *VENTRE À TERRE*

•Abadi, Fthi Arefayne, Joshua Ellul, and George Azzopardi. "The Blockchain of Things, beyond Bitcoin: A Systematic Review." (Abstract, August 2018).

•Allen, Darcy W. E., Chris Berg, Aaron M. Lane, and Jason Potts. "The Economics of Crypto-Democracy." SSRN Electronic Journal, 2017. https://doi.org/10.2139/ssrn.2973050.

•"Bitcoin n-Transactions-Total." Blockchain.com, 2020. https://www.blockchain.com/charts/n-transactions-total.

•BitPay. "What Are Bitcoin Miner Fees?" BitPay Support, April 2020. https://support.bitpay.com/hc/en-us/articles/115003393863-What-are-Bitcoin-miner-fees-.

•Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." (Whitepaper, 2014). https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.

•Cachin, Christian, and Marko Marko Vukolić. "Blockchain Consensus Protocols in the Wild." Cornell University Computer Science. July 7, 2017. https://arxiv.org/abs/1707.01873.

•Chaum, David. “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.”(PhD dissertation, University of California—Berkeley, 1979). https://www.chaum.com/publications/research_chaum_2.pdf.

•Computerphile. “Hashing Algorithms and Security—Computerphile” November 8, 2013. Video, 8:11. https://www.youtube.com/watch?v=b4b8ktEV4Bg

•Featherston, Ed. “Blockchain: You Want Me to Trust a “Trustless Trust” System?” Last Modified November 15th, 2017.https://www.cloudtp.com/doppler/blockchain-you-want-me-to-trust-a-trustless-trust-system/.

•Hankerson, Darrel R., Scott A. Vanstone, and A. J. Menezes. Guide to Elliptic Curve Cryptography. New York: Springer, 2011. 1-15, 75-196.

•“How Many Businesses Accept Bitcoin? Full List (2020).” Fundera, January 1, 2020. https://www.fundera.com/resources/how-many-businesses-accept-bitcoin.

•Katarya, Rahul, and Aamir Mustafa. “Blockchain and Consensus Algorithms.” SSRN Electronic Journal, March 30, 2020. https://doi.org/10.2139/ssrn.3562974.

•Krawisz, Daniel. “The Proof-of-Work Concept.” The Proof-of-Work Concept | Satoshi Nakamoto Institute, June 24, 2013. https://nakamotoinstitute.org/mempool/the-proof-of-work-concept/.

•Leon, Daniel Conte De, Antonius Q. Stalick, Ananth A. Jillepalli, Michael A. Haney, and Frederick T. Sheldon. “Blockchain: Properties and Misconceptions.” Asia Pacific Journal of Innovation and Entrepreneurship 11, no. 3. April 2017. 286–300. https://doi.org/10.1108/apjie-12-2017-034.

•Marr, Bernard. “How Much Data Is There In The World.” Bernard Marr & Co. Intelligent Business Performance (blog), August 2019. https://www.bernardmarr.com/default.asp?contentID=1846.

•Martinez, Julian. “Understanding Proof-of-Work, Part 1: Demystifying Solving a Block.” Medium, May 2018. https://medium.com/@julianrmartinez43/understanding-proof-of-work-part-1-586d7ee6b014.

•Matile, Raphael, and Christian Zurich. “Privacy, Verifiability, and Auditability in Blockchain-Based E-voting.” University of Zurich, Department of Informatics—Communication Systems Group, April 4, 2018. https://files.ifi.uzh.ch/CSG/staff/rodrigues/extern/theses/mp-raphael-christian.pdf.

•Meola, Andrew. “Distributed Ledger Technology & the Blockchain Explained.” Business Insider. January 16, 2020. https://www.businessinsider.com/distributed-ledger-technology-blockchain.

•Nakamato, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System” Satoshi Nakamoto Institute. Last Modified October 31st, 2008. https://nakamotoinstitute.org/Bitcoin/.

•Nakamato, Satoshi. “Re: Slashdot Submission for 1.0.” Satoshi Nakamoto Institute. Last Modified July 5th, 2010. https://satoshi.nakamotoinstitute.org/posts/Bitcointalk/167/.

•Orcutt, Mike. “How Secure Is Blockchain Really?” MIT Technology Review. April 2, 2020. https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.

•SSD, Electronic Frontier Foundation. “A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?” Surveillance Self-Defense, February 19, 2019. https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

•Trubetskoy, Gregory. “Blockchain Proof-of-Work Is a Decentralized Clock—Gregory Trubetskoy.” Gregory Trubetskoy, January 23, 2018. https://grisha.org/blog/2018/01/23/explaining-proof-of-work/.

•Tushar. “How Many Transactions in One Block?” Bitcoin Stack Exchange. April 1, 2015. https://Bitcoin.stackexchange.com/questions/30019/how-many-transactions-in-one-block.

•Y0coin. “Ted Talks: The Blockchain Explained Simply.” December 23rd, 2016. Video, 15:31. https://www.youtube.com/watch?v=KP_hGPQVLpA.

•Zambrano, Brian. “Blockchain Explained: How Does Immutability Work?” VeryPossible, February 27,2018. https://www.verypossible.com/blog/blockchain-explained-how-does-immutability-work.

•Zhang, Shijie, and Jong-Hyouk Lee. “Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network.” IEEE Transactions on Industrial Informatics 15, no. 10. October 2019. 5715–22. https://doi.org/10.1109/tii.2019.2921566.

CHAPTER 2—THE ECONOMICS OF VALUE

•Amadeo, Kimberly. “Why the Dollar Is Worth So Much Less Than It Used to Be.” The Balance. April 13, 2020. https://www.thebalance.com/what-is-the-value-of-a-dollar-today-3306105.

•Annie. “Just 8 Percent of Americans Are Invested in Cryptocurrencies, Survey Says.” CNBC. CNBC, March 16, 2018. https://www.cnbc.com/2018/03/16/why-just-8-percent-of-americans-are-invested-in-cryptocurrencies-.html.

•Banton, Caroline. “The Definition of Economic Value.” Investopedia. January 29, 2020. https://www.investopedia.com/terms/e/economic-value.asp.

•Bitcoin Documentary. Discovery Science Channel / Bitcoin Documentary, 2017. https://www.youtube.com/watch?v=2__yCBGRHVU.

•Brown, Ben, Delton Rhodes, Armin Davis, Rebecca Campbell, and Ana Balashova. “Bitcoin Units and Denominations: A Simple Breakdown From 1 BTC to 1 Satoshi.” BlockExplorer News, September 19, 2018. https://blockexplorer.com/news/Bitcoin-units-denominations/.

•Bruce, Jim. “Money For Nothing—Inside the Federal Reserve.” November 8, 2013. Video, 1:43.00. https://www.youtube.com/watch?v=LkIPiA2QHmI.

•Geller, Martinne. “Toilet Paper Trophy Hunters on a Roll as U.S. Shortages Start Easing.” Reuters. Thomson Reuters, April 29, 2020. https://www.reuters.com/article/us-health-coronavirus-usa-toiletpaper/toilet-paper-trophy-hunters-on-a-roll-as-u-s-shortages-start-easing-idUSKCN22A30A.

•Hostetler, Baker. “COVID-19 Update: Pricing during COVID-19 Without Gouging or Fixing.” JD Supra, April 2020. https://www.jdsupra.com/legalnews/covid-19-update-pricing-during-covid-19-78451/.

•Macleod, Alasdair. “Gold-versus-the-Money-Supply.” Goldmoney. Accessed June 2, 2020. https://www.goldmoney.com/research/goldmoney-insights/gold-versus-the-money-supply.

•Mazikana, Anthony Tapiwa. “The Impact of Cryptocurrencies in Zimbabwe. An Analysis of Bitcoins.” SSRN Electronic Journal, May 24, 2018. https://doi.org/10.2139/ssrn.3376307.

•Menger, Carl. “The Subjective Theory of Value.” Innovator. July 1967, Applications, Experiments, and Advanced Developments of Liberty edition. 38-42.

•Parker, Emily. “Can China Contain Bitcoin?” MIT Technology Review. MIT Technology Review, April 2, 2020. https://www.technologyreview.com/2017/12/11/146816/can-china-contain-Bitcoin/.

•Posch, Anita. “Part 1 Zimbabwe: Ideal Conditions for Bitcoin?—Bitcoin in Africa: The Ubuntu Way.” March 5, 2020. In Bitcoin Co. Podcast, MP3 audio, 48:00. https://www.stitcher.com/podcast/Bitcoin-co/e/68159032?autoplay=true.

•Posch, Anita. “Part 2 Living in a Multi-Currency World—Bitcoin in Africa: The Ubuntu Way.” March 26, 2020. In Bitcoin Co. Podcast, MP3 audio, 43:00. https://www.stitcher.com/podcast/Bitcoin-co/e/68533678?autoplay=true.

•Posch, Anita. "Part 3: Using Bitcoin in Zimbabwe- Bitcoin in Africa: The Ubuntu Way." April 2, 2020. In Bitcoin Co. Podcast, MP3 audio, 43:00. https://www.stitcher.com/podcast/Bitcoin-co/e/68533678?autoplay=true.

•RBI Confirms No Ban on Cryptocurrency Exchanges. "US Lawmaker Introduces Crypto-Currency Act of 2020 While Under Coronavirus Quarantine: Regulation Bitcoin News." Bitcoin News, March 10, 2020. https://news.Bitcoin.com/cryptocurrency-act-of-2020/.

•Reynold, Stark. "Cryptoeconomics Vitalik Buterin—The Best Documentary Ever" December 5th, 2017. Video, 54:23. https://www.youtube.com/watch?v=2xS8zd1POGM.

•Rosic, Ameer. "What Is Cryptocurrency? [Everything You Need To Know!]." Blockgeeks, May 5, 2020. https://blockgeeks.com/guides/what-is-cryptocurrency/.

•Satoshi. "Warren Buffett Slates Bitcoin, Denies Owning Crypto Gifted by Justin Sun: Featured Bitcoin News." Bitcoin News, February 24, 2020. https://news.Bitcoin.com/warren-buffett-denies-owning-crypto/.

•Senator Carper. "Chairman Carper Opening Statement at Senate Committee Hearing on Virtual Currency." November 18th, 2013. Video, 10:40. https://www.youtube.com/watch?v=x8Y71IXEK8w.

•"Total-Bitcoins." Blockchain.com. Accessed June 2, 2020. https://www.blockchain.com/charts/total-Bitcoins.

•Varian, Hal R. "Why Is That Dollar Bill in Your Pocket Worth Anything?" The New York Times, January 15, 2004.

CHAPTER 3: DIGITAL PIONEERS—THE STORIES OF DECENTRALIZATION

•Andres, Tommy. "Divided Decade: How the Financial Crisis Changed Jobs." Marketplace, April 29, 2019. https://www.marketplace.org/2018/12/19/what-we-learned-jobs/.

•Armstrong, Brian. "What Happened in Crypto over the Last Decade." Medium. The Coinbase Blog, March 5, 2020. https://blog.coinbase.com/what-happened-in-crypto-over-the-last-decade-ee6a2552d630.

•Bernard, Zoë. "Everything You Need to Know about Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of Its Creator." Business Insider. Business Insider, November 10, 2018. https://www.businessinsider.com/Bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.

•Bitcoin. "Bitcoin Github Repository." GitHub, June 1, 2020. https://github.com/Bitcoin/Bitcoin.

- "Bitcoin n-Transactions-Total." Blockchain.com, 2020. https://www.blockchain.com/charts/n-transactions-total.

- Blagdon, Jeff. "Technical Problems Cause Bitcoin to Plummet from Record High, Mt. Gox Suspends Deposits." The Verge. March 12, 2013. https://www.theverge.com/2013/3/12/4092898/technical-problems-cause-Bitcoin-to-plummet-from-record-high.

- Canellis, David. "Satoshi Nakamoto Left Bitcoin Because of the CIA, a Theory." Hard Fork | The Next Web, July 19, 2019. https://thenextweb.com/hardfork/2019/07/19/satoshi-nakamoto-left-Bitcoin-because-of-the-cia-theory-cryptocurrency/.

- Chen, Adrian. "Massive Bitcoin Business Partnership Devolves Into $75 Million Lawsuit." Gawker. May 2, 2013. https://gawker.com/massive-Bitcoin-business-partnership-devolves-into-75-487857656?rev=1367540238.

- Distributed. "Distributed 2018: Keynote Presentation—David Chaum." August 20, 2018. Video, 25:01. https://www.youtube.com/watch?v=2YtqVSxa3aI&t=655s.

- Epicenter Podcast. "David Chaum: The Forefather of Cryptocurrencies and the Cypherpunk Movement (#304)." September 10, 2019. Video, 1:03.57. https://www.youtube.com/watch?v=LkIPiA2QHmI.

- "Ethereum Sharding Explained: Understanding Ethereum." district0x Education Portal. Accessed June 2, 2020. https://education.district0x.io/general-topics/understanding-ethereum/ethereum-sharding-explained/.

- Floyd, David. "10 Years After Lehman: Bitcoin and Wall Street Are Closer Than Ever." CoinDesk. CoinDesk, September 13, 2018. https://www.coindesk.com/10-years-after-lehman-Bitcoin-and-wall-street-are-closer-than-ever.

- Floyd, David. "Genesis Block: Chancellor on Brink of Second Bailout for Banks · Monnos." Monnos, April 15, 2020. https://monnos.com/en/blog/genesis-block-chancellor-on-brink-of-second-bailout-for-banks/.

- "Global Bitcoin Nodes Distribution." Bitnodes, June 2, 2020. https://bitnodes.io/nodes/.

- Jeffries, Adrianne. "Inside the Bizarre Upside-down Bankruptcy of Mt. Gox." The Verge. March 22, 2018. https://www.theverge.com/2018/3/22/17151430/bankruptcy-mt-gox-liabilities-Bitcoin.

- Li, Kenny. "The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed." Hacker Noon, June 1, 2020. https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44.

•Lielacher, Alex. “Why Has Satoshi Nakamoto Remained Anonymous?” Brave New Coin, April 15, 2018. https://bravenewcoin.com/insights/why-has-satoshi-nakamoto-remained-anonymous.

•McCullagh, Declan. “Homeland Security Cuts off Dwolla Bitcoin Transfers.” CNET. CNET, May 14, 2013. https://www.cnet.com/news/homeland-security-cuts-off-dwolla-Bitcoin-transfers/.

•Mechkaroska, Daniela, and Aleksandra Popovska-Mitrovikj. “Analysis of the Possibilities for Improvement of BlockChain Technology.” Telecommunications Forum (TELFOR), November 26, 2018, 1–4. https://doi.org/10.1109/TELFOR.2018.8612034.

•Michael Noel. “Vitalik Buterin The Boy Genius Behind Ethereum.” November 8, 2017. Video, 59:55. https://www.youtube.com/watch?v=irr8Au_unnE.

•Moore, Galen. “10 Years On, Laszlo Hanyecz Has No Regrets About His $45M Bitcoin Pizzas.” CoinDesk. CoinDesk, May 22, 2020. https://www.coindesk.com/Bitcoin-pizza-10-years-laszlo-hanyecz.

•Nakamoto, Satoshi. “Bitcoin Open Source Implementation of P2P Currency: Satoshi Nakamoto Institute.” Bitcoin open source implementation of P2P currency | Satoshi Nakamoto Institute, February 11, 2009. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

•Nelson, Danny, and Nikhilesh De. “Coinbase Broke Traffic Records and Saw Massive Volume During Market Collapse.” CoinDesk, March 20, 2020. https://www.coindesk.com/coinbase-broke-traffic-records-and-saw-massive-volume-during-market-collapse.

•Noah, James. “Mt. Gox Interviews: Jed McCaleb on the Creation of Mt. Gox.” Hacker Noon, February 26, 2019. https://hackernoon.com/mt-gox-interviews-jed-mccaleb-on-the-creation-of-mt-gox-f1f0563cf892.

•Norry, Andrew. “The History of the Mt Gox Hack: Bitcoin’s Biggest Heist.” Blockonomi, March 31, 2020. https://blockonomi.com/mt-gox-hack/.

•Ometoruwa, Toju. “Solving the Blockchain Trilemma: Decentralization, Security & Scalability.” Coin Bureau, June 12, 2018. https://www.coinbureau.com/analysis/solving-blockchain-trilemma/#:~:text=The ‘Scalability Trilemma’ is a,security, without compromising either one.&text=Security (defined as being secure,to O(n) resources).

•Paybis. “How Many Blockchain Developers Are There In 2020?” Paybis Blog, May 18, 2020. https://paybis.com/blog/how-many-blockchain-developers-are-there/.

•Peck, Morgan. “The Uncanny Mind That Built Ethereum.” Wired. Conde Nast, June 16, 2017. https://www.wired.com/2016/06/the-uncanny-mind-that-built-ethereum/.

•Popper, Nathaniel. “How Mt. Gox Imploded.” Vice, May 19, 2015. https://www.vice.com/en_us/article/ae38qb/how-mt-gox-imploded.

•Popper, Nathaniel. “The People Leading the Blockchain Revolution.” The New York Times. The New York Times, June 28, 2018. https://www.nytimes.com/2018/06/27/business/dealbook/blockchain-stars.html.

•Sfox. “Bitcoin Governance: What Are BIPs and How Do They Work?” SFOX Edge, April 16, 2019. https://www.sfox.com/blog/Bitcoin-governance-what-are-bips-and-how-do-they-work/.

•“The Decentralized Dream, Realized.” Elixxir. Accessed June 2, 2020. https://elixxir.io/.

•Walters, Joanna. “Occupy America: Protests against Wall Street and Inequality Hit 70 Cities.” The Guardian. Guardian News and Media, October 8, 2011. https://www.theguardian.com/world/2011/oct/08/occupy-america-protests-financial-crisis.

•Wang, Kyle. “Ethereum: Turing-Completeness and Rich Statefulness Explained.” Hacker Noon, June 1, 2020. https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb.

CHAPTER 4: USE CASES—SYNERGY & FINAL FRONTIERS

•Art of the Problem. “Public key cryptography—Diffie-Hellman Key Exchange (full version).” July 30, 2012. Video, 8:37. https://www.youtube.com/watch?v=YEBfamv-_do.

•BitDegree. “What Is a Smart Contract and How Do Smart Contracts Work.” BitDegree Tutorials. BitDegree, January 21, 2020. https://www.bitdegree.org/tutorials/what-is-a-smart-contract/.

•“Blockchain Use Cases in 2020: Real World Industry Applications.” ConsenSys. Accessed June 1, 2019. https://consensys.net/blockchain-use-cases/.

•Blockgeeks. “Real World Blockchain Applications—Healthcare.”“ February 22, 2019. 5:04. https://www.youtube.com/watch?v=md0K6nGewTU.

•Cecchetti, Steve, and Kim Schoenholtz. “The Stubbornly High Cost of Remittances.” Money, Banking and Financial Markets. Money, Banking and Financial Markets, February 19, 2018. https://www.moneyandbanking.com/commentary/2018/2/18/the-stubbornly-high-cost-of-remittances.

•Cohan, Peter. “Big Risk: $1.2 Quadrillion Derivatives Market Dwarfs World GDP.” AOL.com. AOL, July 15, 2016. https://www.aol.com/2010/06/09/risk-quadrillion-derivatives-market-gdp/.

•Hoar, Sean. “Identity Theft: The Crime of the New Millennium.” HeinOnline, 2001. https://heinonline.org/HOL/LandingPage?handle=hein.journals/orglr80&div=34&id=&page=.

•Insurance Information Institute. “Facts Statistics: Identity Theft and Cybercrime.” III, January 2018. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

•Jensen, Kurt. “More Data More Problems: Fixing EHRs and Information Blocking in Healthcare.” Health Professions Network, February 20, 2020. https://hpnonline.org/more-data-more-problems-fixing-ehrs-and-information-blocking-in-healthcare/.

•Kennedy, Shirley. “Your Password Has Expired and Must Be Changed.” Information Today, Inc., April 2016. http://www.infotoday.com/IT/apr16/Kennedy--Your-Password-Has-Expired-and-Must-Be-Changed.shtml#:~:text=According to an often-quoted,papers/www2007.pdf).

•Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado. “Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications.” Journal of the American Medical Informatics Association 24, no. 6 (August 2017): 1211–20. https://doi.org/10.1093/jamia/ocx068.

•M., Casey, J. Crane, G. Gensler, S. Johnson and N. Narula. “The Impact of Blockchain Technology and Finance: A Catalyst for Change.” Geneva Report on the World Economy No. 21, 2018.

•Melrose, Lyndel. “A Blueprint for Digital Identity: Deloitte Papua New Guinea: Financial Services.” Deloitte Australia, November 7, 2017. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-blueprint-digital-identity-150816.pdf.

•Monica, Kate. “Regenstrief to Develop Automated Patient EHR Matching Solution.” EHRIntelligence, August 14, 2017. https://ehrintelligence.com/news/regenstrief-to-develop-automated-patient-ehr-matching-solution.

•Moskov, alex. “What Is Ripple (XRP)?: A Complete Guide to the Banking Cryptocurrency.” CoinCentral, May 29, 2020. https://coincentral.com/what-is-ripple-xrp/.

•Nikolova, Maria. “ASX Takes Its Investment in Digital Asset to $30.9m.” FinanceFeeds, December 13, 2019. https://financefeeds.com/asx-takes-investment-digital-asset-30-

9m/.

- "Nostro Account—Overview, How It Works, Example." Corporate Finance Institute. Accessed June 2, 2020. https://corporatefinanceinstitute.com/resources/knowledge/finance/nostro-account/.

- "Only 48% of ICOs Were Successful Last Year—but Startups Still Managed to Raise $5.6 Billion | Currency News | Financial and Business News | Markets Insider." Business Insider. Business Insider. Accessed June 2, 2020. https://markets.businessinsider.com/currencies/news/how-much-raised-icos-2017-tokendata-2017-2018-1-1014647330.

- Randall, David, Pradeep Goel, and Ramzi Abujamra. "Blockchain Applications and Use Cases in Health Information Technology." Journal of Health & Medical Informatics 08, no. 03 (2017). https://doi.org/10.4172/2157-7420.1000276.

- Robinson, Edward, and Matthew Leising. "Blythe Masters Tells Banks the Blockchain Changes Everything." Bloomberg.com. September 1, 2015. https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything.

- SelfKey Foundation. "Self Key." (Whitepaper, September 11, 2017). https://selfkey.org/wp-content/uploads/2019/03/selfkey-whitepaper-en.pdf.

- "Sending Money Back Home." Clovr. Clovr, February 24, 2020. https://www.clovr.com/page/sending-money-back-home/.

- Su, Eva. Accredited investor definition and private securities markets, Accredited investor definition and private securities markets § (n.d.).

- Szabo, Nick. "The Idea Of Smart Contracts." Nick Szabo. Accessed June 2, 2020. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

- "Venture Capital Vs Business Loans: A Beginner's Guide to Financing Alternatives." Business Funding, Working Capital Loans, Small Business Loans, March 13, 2019. https://www.mulliganfunding.com/blog/venture-capital-vs-business-loans-a-beginners-guide-to-financing-alternatives/.

- Zuckerman, Molly Jane. "Ripple CEO Talks Liquidity And Regulation: Ultimately Governments Aren't Going Away." Cointelegraph. Cointelegraph, March 6, 2018. https://cointelegraph.com/news/ripple-ceo-talks-liquidity-and-regulation-ultimately-governments-arent-going-away.

CHAPTER 5: ON LOSS AND HOW IT HAPPENS

•Adamczyk, Alicia. "Index Funds Are More Popular than Ever-Here's Why They're a Smart Investment." CNBC. September 19, 2019. https://www.cnbc.com/2019/09/19/why-index-funds-are-a-smart-investment.html.

•Benz, Christine. "How to Benchmark Your Portfolio." Morningstar, Inc., February 25, 2019. https://www.morningstar.com/articles/915208/how-to-benchmark-your-portfolio.

•BluFX. "What Is Trading Psychology?" BluFX Blog. Accessed June 21, 2020. https://blog.blufx.co.uk/what-is-trading-psychology.

•Edspira. "Time Value of Money (Concept Explained)." September 17th, 2013. Video, 7:00. https://www.youtube.com/watch?v=gkoEAPAW7eg.

•Fitzpatrick, Luke. "The Tipping Point For Mass Blockchain Adoption." Forbes. Forbes Magazine, September 3, 2019. https://www.forbes.com/sites/lukefitzpatrick/2019/08/21/the-tipping-point-for-mass-blockchain-adoption/#25d3bbfd5736.

•Franklin, Phillip, Thomas Andrews, Eva Hart, and Lawrence Beesley. "The Titanic—Quotes From Survivors." The Titanic. Accessed June 2, 2020. https://thetitanicnhdproject.weebly.com/quotes-from-survivors.html.

•"I'm Always Thinking about Losing Money as Opposed to Making Money." Valens Research, March 29, 2019. https://www.valens-research.com/im-always-thinking-about-losing-money-as-opposed-to-making-money/.

•Marginal Revolution University."What Is Opportunity Cost?" August 14th, 2018. Video, 2:45. https://www.youtube.com/watch?v=x-hYzRncxTc.

•Rob P. Gekwiak. "Lost Money Investing in Cryptocurrency." August 30, 2016. Video, 5:01. https://www.youtube.com/watch?v=IWeudZaC7po.

•SophonEX. "Does Cryptocurrency Have More Black Swan Events than Other Assets?" Medium. SophonEX, March 3, 2019. https://medium.com/sophonexchange/does-cryptocurrency-have-more-black-swan-events-than-other-assets-c274ad26a5c

CHAPTER 6: INVESTING PSYCHOLOGY—THE RIGHT & WRONG

•Alkhars, Mohammed, Nicholas Evangelopoulos, Robert Pavur, and Shailesh Kulkarni. "Cognitive Biases Resulting from the Representativeness Heuristic in Operations Management: an Experimental Investigation."Psychology Research and Behavior Management Volume 12. April 10, 2019. 263–76. https://doi.org/10.2147/prbm.s193092.

- Bhala, Kara Tan, Warren Yeh, and Raj Bhala. International Investment Management: Theory, Ethics and Practice. London: Routledge, Taylor & Francis Group, 2016. 45.

- Cureen Capital. "Investment Journals: Not for the Weak." June 4, 2019. Video, 13:12.

- Elton, Edwin J., Martin J. Gruber, and Christopher R. Blake. "Survivor Bias and Mutual Fund Performance." Review of Financial Studies 9, no. 4 (1996): 1097–1120. https://doi.org/10.1093/rfs/9.4.1097.

- Gal, David. "What Does Loss Aversion Mean for Investors?" Psychology Today. Sussex Publishers, May 16, 2019. https://www.psychologytoday.com/us/blog/the-power-the-status-quo/201905/what-does-loss-aversion-mean-investors.

- Grohol, John M. "FOMO Addiction: The Fear of Missing Out." World of Psychology, July 8, 2018. https://psychcentral.com/blog/fomo-addiction-the-fear-of-missing-out/.

- Grohol, John M. "Why 'Sleeping on It' Helps." LiveScience. Purch, October 26, 2009. https://www.livescience.com/5820-sleeping-helps.html.

- Hoffstein, Corey. "Investors Beware the House Money Effect." Forbes. Forbes Magazine, January 21, 2016. https://www.forbes.com/sites/greatspeculations/2015/08/31/investors-beware-the-house-money-effect/. https://www.youtube.com/watch?v=UE6ZMud2-9Y.

- Kahneman, Daniel. Thinking, Fast and Slow. Random House, 2011. 426.

- Kaplan, Michael. "Bitcoin Crash: This Man Lost His Savings When Cryptocurrencies Plunged." CNNMoney. Cable News Network, September 11, 2018. https://money.cnn.com/2018/09/11/investing/Bitcoin-crash-victim/index.html.

- Kumar, Sweeny. "Anchoring Bias And Their Effects On Investment Decisions Series—Part 10." ValueWalk, February 1, 2020. https://www.valuewalk.com/2018/08/behavioral-anchoring-bias/.

- Kumar, Sweeny. "Behavioural Biases and Their Effects on Investment Decisions Series—Part 3." ValueWalk, February 1, 2020. https://www.valuewalk.com/2018/07/overconfidence-bias-investing/.

- Richards, Anthony J. "Winner-Loser Reversals in National Stock Market Indices: Can They Be Explained?" IMF Working Papers 97, no. 182 (1997): 1. https://doi.org/10.5089/9781451859232.001.

- Royce IP. "The Conjunctive and Disjunctive Events Bias." Farnam Street, January 18, 2016. https://fs.blog/2011/11/mental-model-conjunctive-and-disjunctive-events-bias/.

- "Sample Size Fallacy." Oxford Reference. Accessed June 3, 2020. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100439475.

•Shefrin, Hersh. "Beyond Greed and Fear: Understanding Behavioral Finance and the Psychology of Investing." Oxford: Oxford University Press, 2007.

•Vakkur. "Behavioral Finance—Evidence For Heuristics." Behavioral finance. Accessed June 3, 2020. http://www.vakkur.com/hx/beh_fin_sum.htm.

CHAPTER 7: ON WORDS FROM THE WISE

•Chen, James. "Risk." Investopedia. Investopedia, March 27, 2020. https://www.investopedia.com/terms/r/risk.asp.

•Efrat. "Efrat Cybulkiewicz." America-Israel Cultural Foundation, April 26, 2019. https://aicf.org/artist/efrat-cybulkiewicz/.

•Erasmus, Desiderius. Adagia. Basileae: In aedibus Ioannis Frobenii, mense Octobri, 1520.

•Franklin, Benjamin, Lewis F. White, John DePol, and Bruce Rogers. The Way to Wealth: Preface to Poor Richard Improved, 1758. New York, 1953.

•Galloway, Scott. "An Economic Bubble Is about to Burst, and These Are the Very Clear Warning Signs." Business Insider. Business Insider, May 30, 2019. https://www.businessinsider.com/warning-signs-that-an-economic-bubble-is-about-to-burst-2019-5.

•Stocktwits. "The Parabolic Arc Pattern or How To Profit from Euphoria and Bubbles." Medium. The Stocktwits Blog, May 18, 2017. https://blog.stocktwits.com/the-parabolic-arc-pattern-or-how-to-profit-from-euphoria-and-bubbles-a732cc750c2b.

•"Top Anecdotal Signs of a Market Bubble." bmcamcom, September 9, 2017. https://bmc-am.com/top-anecdotal-signs-of-a-market-bubble/.

CHAPTER 8: PRINCIPLES

•Abraham, Stephan A. "5 Popular Portfolio Types." Investopedia. Investopedia, April 13, 2020. https://www.investopedia.com/articles/basics/11/5-popular-portfolio-types.asp.

•Arnuphaptrairong, Tharwon. "Top Ten Lists of Software Project Risks : Evidence from the Literature Survey." IMECS 1 (March 16, 2011).

•Chang, Ellen. "What to Know About Investment Fees." U.S. News & World Report. U.S. News & World Report, March 3, 2020. https://money.usnews.com/investing/investing-101/articles/what-to-know-about-investment-fees.

•Chappelow, Jim. "Savings Rate." Investopedia. Investopedia, March 10, 2020. https://www.investopedia.com/terms/s/savings-rate.asp.

•Chorpenning, Ashley. "Why Time Horizons Matter in Investing." SmartAsset. SmartAsset, January 8, 2020. https://smartasset.com/investing/time-horizon.

•Fischer, Ben. "Kathryn Minshew: The 'Wizardess of Oz'." bizjournals.com, April 4, 2014. https://www.bizjournals.com/bizwomen/news/profiles-strategies/2014/04/kathryn-minshew-the-wizardesse-of-oz.html?page=all.

•Ferri, Rick. "Six Rules to Disciplined Investing." Forbes. Forbes Magazine, April 24, 2018. https://www.forbes.com/sites/rickferri/2015/10/06/six-rules-to-disciplined-investing/.

•Kennon, Joshua. "Dollar Cost Averaging Explained."The Balance. December 2, 2019. https://www.thebalance.com/dollar-cost-averaging-356331.

•Movement Capital. "Value Averaging: An Alternative to DCA or Lump Sum." Movement Capital, December 3, 2019. https://movement.capital/value-averaging-an-alternative-to-dollar-cost-averaging-or-lump-sum/.

•Rosenberg, Eric. "The Case Against Rebalancing Your Portfolio." The Balance. The Balance, April 6, 2020. https://www.thebalance.com/the-case-against-rebalancing-your-portfolio-4160045.

•Thayqua. "Warren Buffett: How to Pick Stocks & Get Rich (1985)." January 16, 2018. Video, 6:28. https://www.youtube.com/watch?v=PEs5caq8QNs.

•"The Most Important Determinant of Investment Returns." Index Fund Advisors, Inc.—Fiduciary Wealth Services, DFA Funds. Accessed February 7, 2018. https://www.ifa.com/articles/The_Most_Important_Determinant_of_Investment_Returns/.

•"Vanguard Principles for Investing Success." Vanguard Investing, 2017. https://about.vanguard.com/what-sets-vanguard-apart/principles-for-investing-success/ICRPRINC_042017_Online.pdf.

•"What Is Portfolio Diversification?" Fidelity. Accessed June 4, 2020. https://www.fidelity.com/learning-center/investment-products/mutual-funds/diversification.

CHAPTER 9: QUALITATIVE ANALYSIS—RISK

•Bloomberg, Jason. "Seven Lies ICO Fans Tell Themselves (And Anyone Else Who Will Listen)." Forbes. Forbes Magazine, June 29, 2018. https://www.forbes.com/sites/jasonbloomberg/2018/06/29/seven-lies-ico-fans-tell-themselves-and-anyone-else-who-will-listen/.

•Brooks, Frederick Phillips. The Mythical Man-Month Essays on Software Engineering. Boston, MA: Addison-Wesley, 2013.

•Caspian. "The Four Barriers For Institutions Entering Crypto." Medium. Caspian.tech Blog, July 8, 2018. https://medium.com/caspian-tech/what-are-the-main-barriers-for-institutions-entering-crypto-e96aef30d462.

•CFI. "Liquidity—Definition, Example, Market vs Accounting Liquidity." Corporate Finance Institute, February 26, 2020. https://corporatefinanceinstitute.com/resources/knowledge/finance/liquidity/.

•Chorpenning, Ashley. "What Is a Risk Profile?" SmartAsset. SmartAsset, January 31, 2020. https://smartasset.com/financial-advisor/risk-profile.

•Edwards, Ian. "Boom, Bust and Blockchain: RChain Cooperative's Cryptocurrency Dreams Dissolve into Controversy." GeekWire, February 28, 2019. https://www.geekwire.com/2019/boom-bust-blockchain-rchain-cooperatives-cryptocurrency-dreams-dissolve-controversy/.

•Jenkinson, Gareth. "Bitconnect Ponzi Scheme—No Sympathy From Crypto Community." Cointelegraph. Cointelegraph, January 19, 2018. https://cointelegraph.com/news/bitconnect-ponzi-scheme-no-sympathy-from-crypto-community.

•Johnston, Kevin. "The Concepts of Return on Investment & Risk." Small Business—Chron.com. October 26, 2016. https://smallbusiness.chron.com/concepts-return-investment-risk-68026.html.

•Kenton, Will. "The Ins and Outs of Business Risk." Investopedia. Investopedia, February 5, 2020. https://www.investopedia.com/terms/b/businessrisk.asp.

•Moos, Mitchell. "RChain Cooperative May Need to Liquidate RHOC Holdings to Remain Solvent." CryptoSlate, September 11, 2019. https://cryptoslate.com/rchain-cooperative-may-need-to-liquidate-rhoc-holdings-to-remain-solvent/.

•Orsini, Lauren, and Code. "GitHub For Beginners: Don't Get Scared, Get Started." ReadWrite, July 26, 2018. https://readwrite.com/2013/09/30/understanding-github-a-journey-for-beginners-part-1/.

•Poveda-Bautista, Rocio, Jose-Antonio Diego-Mas, and Diego Leon-Medina. "Measuring the Project Management Complexity: The Case of Information Technology Projects." Complexity. 2018. 1–19. https://doi.org/10.1155/2018/6058480.

•Prince, Dan. "Project Complexity: What Makes Software Development Complex . . . and How Your Developer Can Make It Easier ." illumisoft. Illumisoft, August 8, 2018.

https://illumisoft.com/project-complexity/.

•"Qualitative vs Quantitative Analysis." Investing.com, March 9, 2012. https://www.investing.com/analysis/qualitative-vs-quantitative-analysis-116495.

•Shepherd, Maddie. "ICO Statistics (2020): Funding, Investment, and Best ICOs." Fundera, December 31, 2019. https://www.fundera.com/resources/ico-statistics.

•Smigel, Leo. "Slippage: What It Is & How to Avoid It." Analyzing Alpha. Analyzing Alpha, November 29, 2019. https://analyzingalpha.com/slippage.

•Thakur, Dinesh. "Dinesh Thakur." Computer Notes. Accessed June 4, 2020. http://ecomputernotes.com/software-engineering/softwarerequirement.

•Torbati, Yuval, David Bodek, and Mark Puccia. "Methodology: Industry Risk." Ratings Direct. S&P Global Ratings, 2016. https://www.maalot.co.il/Publications/MT20161215151239.pdf.

•Zerucha, Tony. "Skills Shortage Hurting Blockchain Growth? Industry Weighs In." Bankless Times, April 19, 2018. https://www.banklesstimes.com/2018/04/18/skills-shortage-hurting-blockchain-growth-industry-weighs-in/.

•Zwanenburg Decentralization, Jorn van. "7 Signs of Bad Cryptocurrency." Invest In Blockchain, November 1, 2017. https://www.investinblockchain.com/7-signs-bad-cryptocurrency/.

CHAPTER 10: NARRATIVE

•Cotto, Andrew. "A Conversation With Dennis Lehane." grubstreet, January 10, 2012. https://grubstreet.org/blog/a-conversation-with-dennis-lehane/.

•Damodaran, Aswath. *Narrative And Numbers: the Value of Stories in Business*. HarperCollins India, 2018.

•"Home." Golem. Accessed June 4, 2020. https://golem.network/.

CHAPTER 11: QUANTITATIVE MODELS & METRICS—ERROR OF PROJECTION

•Binance Academy. "Proof of Stake Explained." Binance Academy. January 19, 2020. https://academy.binance.com/blockchain/proof-of-stake-explained.

•"Charts." Coin Metrics. Accessed June 4, 2020. https://coinmetrics.io/charts/.

•"Discounted Cash Flow DCF Formula—Guide How to Calculate NPV." Corporate Finance Institute, October 22, 2019. https://corporatefinanceinstitute.com/resources/knowledge/valuation/dcf-formula-guide/.

•Ernst & Young. "The Valuation of Crypto-Assets," 2019. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-the-valuation-of-crypto-assets.pdf.

•"Ethereum Transactions Per Day:" YCharts. Accessed June 4, 2020. https://ycharts.com/indicators/ethereum_transactions_per_day.

•Fawkes, Jeff. "The 8 Most Important Cryptocurrency Metrics to Look For." Bitsonline, February 1, 2019. https://bitsonline.com/8-important-cryptocurrency-metrics/.

•Karamat, Sheba. "How Are Crypto Prices Determined?—Cryptocurrency Guide." Coin Rivet, March 23, 2019. https://coinrivet.com/guides/what-is-cryptocurrency/how-cryptocurrencies-maintain-their-prices/.

•Kim, Daniel Sangyoon. "Fundamentally Valuing Bitcoin at $45,000 / BTC." Hacker Noon, May 4, 2020. https://hackernoon.com/fundamentally-valuing-Bitcoin-at-45-000-btc-a7f171521ae6.

•Kuznetsov, Nikolai. "Ethereum 2.0 Staking, Explained." Cointelegraph. Cointelegraph, May 25, 2020. https://cointelegraph.com/explained/ethereum-20-staking-explained.

•"Quantitative Analysis—Definition, Techniques and Applications." Corporate Finance Institute, February 19, 2020. https://corporatefinanceinstitute.com/resources/knowledge/finance/quantitative-analysis/.

•Rao, Leena. "PayPal Now Processing $315 Million In Payments Per Day." TechCrunch. TechCrunch, September 25, 2011. https://techcrunch.com/2011/09/25/paypal-now-processing-315-million-in-payments-per-day/.

•Seth, Shobhit. "Why NEO Can Do What No Other Cryptocurrency Can Do." Investopedia. Investopedia, January 29, 2020. https://www.investopedia.com/tech/china-neo-cryptocurrency/.

CHAPTER 12: ENTRY & EXIT

•"Community Network Data." Coin Metrics. Accessed June 4, 2020. https://coinmetrics.io/community-network-data/.

•"Cryptocurrencies." MarketWatch. Accessed January 12, 2019. https://www.marketwatch.com/investing/cryptocurrency/.

•Goldfarb, and David A Kirsch. "Economic Bubbles Are Irrational, but We Can Understand Them—Brent Goldfarb & David A Kirsch: Aeon Essays." Aeon. Aeon, June 4, 2020. https://aeon.co/essays/economic-bubbles-are-irrational-but-we-can-understand-them.

•InvestorsLive. "[Weekly Lesson] Why Timing Is the Most Important Factor in Trading." Investors Underground, February 11, 2020. https://www.investorsunderground.com/timing-in-trading/.

•Lefèvre Edwin. *Reminiscences of a Stock Operator*. Mineola: Ixia Press, 2018.

•Stapel, Elizabeth. "Mean, Median, Mode, and Range." Purplemath. Accessed June 4, 2020. https://www.purplemath.com/modules/meanmode.htm.

•Stocktwits, Inc. "The Importance of Setting a Stop Loss and What It Means to Traders and Investors." Medium. The Stocktwits Blog, July 22, 2016. https://blog.stocktwits.com/the-importance-of-setting-a-stop-loss-and-what-it-means-to-traders-and-investors-bceb360b2a2e.

•"What Is SMA?—Simple Moving Average." Fidelity, 2009. https://www.fidelity.com/learning-center/trading-investing/technical-analysis/technical-indicator-guide/sma.

CHAPTER 13: TAXATION & REGULATION

•Anderson, Matt, Bazil, Jeff, Alex, Malcolm, John, Jessa, and Firo Solutions. "Who Accepts Bitcoins in 2020? List of 20+ Major Companies." 99 Bitcoins. Accessed June 4, 2020. https://99Bitcoins.com/Bitcoin/who-accepts/.

•Avan-Nomayo, Osato. "Cryptocurrency Mixers and Why Governments May Want to Shut Them Down." Cointelegraph. Cointelegraph, May 28, 2019. https://cointelegraph.com/news/cryptocurrency-mixers-and-why-governments-may-want-to-shut-them-down.

•BitTrust. "Passing the Howey Test: How to Regulate Blockchain Tokens." Medium. BitTrust, March 4, 2017. https://medium.com/bittrust/passing-the-howey-test-how-to-regulate-blockchain-tokens-d218da93a8b6.

•Center, Coin. "Today in Congress Rep. Sherman Called for a Bill to Ban All Cryptocurrencies." Twitter. Twitter, May 9, 2019. https://twitter.com/coincenter/status/1126574631605997569.

•Chen, James. "Capital Gain." Investopedia. Investopedia, January 29, 2020. https://www.investopedia.com/terms/c/capitalgain.asp.

•Constine, Josh. "Facebook Announces Libra Cryptocurrency: All You Need to Know." TechCrunch. TechCrunch, June 18, 2019. https://techcrunch.com/2019/06/18/facebook-libra/.

•Costine, Josh. "Facebook Crypto Consortium Libra Association Has Lost 8 'Founding Members'." Yahoo! Finance. Yahoo!, October 11, 2019. https://finance.yahoo.com/news/facebook-crypto-libra-association-collapsing-founding-members-drop-out-paypal-ebay-mastercard-203709438.html.

•CryptoTrader Tax. "Crypto & Bitcoin Taxes Explained—Everything You Need To Know | CryptoTrader.Tax." July 31, 2019. Video, 11:56. https://www.youtube.com/watch?v=K0zT29RwbGE&feature=emb_logo.

•De, Nikhilesh. "ICO Project Enigma Settles SEC Charges Over $45M Token Sale." CoinDesk. CoinDesk, February 19, 2020. https://www.coindesk.com/ico-project-enigma-settles-sec-charges-over-45m-token-sale.

•El-Sibaie, Amir. "2020 Tax Brackets." Tax Foundation, March 13, 2020. https://taxfoundation.org/2020-tax-brackets/.

•Enigma Project. "Introducing Secret Network." Medium. Enigma, May 27, 2020. https://blog.enigma.co/introducing-secret-network-ed48621754ad.

•Fields, Carlton. "State Regulations on Virtual Currency and Blockchain Technologies—(Updated)." JD Supra, April 19, 2019. https://www.jdsupra.com/legalnews/state-regulations-on-virtual-currency-97006/.

•"Gift Tax." Internal Revenue Service. Accessed June 4, 2020. https://www.irs.gov/businesses/small-businesses-self-employed/gift-tax.

•Gilbert, Christine. "Blockchain Technology Act." SB0213, May 14, 2019. https://le.utah.gov/~2019/bills/static/SB0213.html.

•Gosar, Paul. "Text—H.R.6154—116th Congress (2019-2020): Crypto-Currency Act of 2020." Congress.gov, March 9, 2020. https://www.congress.gov/bill/116th-congress/house-bill/6154/text?q=%7B%22search%22%3A%5B%22crypto-currency+act%22%5D%7D.

•"HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency." Business Wire, January 15, 2020. https://www.businesswire.com/news/home/20200115005482/en/HSB-Survey-Finds-One-Third-Small-Businesses-Accept.

•"International Legal Business Solutions—Global Legal Insights." GLI—Global Legal InsightsInternational legal business solutions. Global Legal Group. Accessed December

17, 2019. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa.

•IRS. "Notice 2014-21." https://www.irs.gov/pub/irs-drop/n-14-21.pdf, April 14, 2014.

•Kemmerer, David. "The 2020 Guide To Cryptocurrency Taxes." RSS, January 2020. https://cryptotrader.tax/blog/the-traders-guide-to-cryptocurrency-taxes.

•Kim, Robert. "Analysis: A Crypto-Currency Act of 2020? You Cannot Be Serious!" Bloomberg BNA News, January 13, 2020. https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-a-crypto-currency-act-of-2020-you-cannot-be-serious.

•Kooney, Kate. "SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies." CNBC. CNBC, June 11, 2018. https://www.cnbc.com/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html.

•Morse, Andrew. "What You Need to Know about Facebook's Libra Cryptocurrency." CNET, October 24, 2019. https://www.cnet.com/news/heres-what-you-need-to-know-about-facebooks-controversial-libra-cryptocurrency/.

•Pines, Lawrence. "Electricity: Learn How To Trade It at Commodity.com." Commodity.com, August 16, 2019. https://commodity.com/energy/electricity/.

•"Press Release." SEC Emblem, February 19, 2020. https://www.sec.gov/news/press-release/2020-37.

•"SEC v. Howey Co., 328 U.S. 293 (1946)." Justia Law. Accessed June 4, 2020. https://supreme.justia.com/cases/federal/us/328/293/.

•thoway. "r/Personalfinance—I Just Discovered That I Owe the IRS $50k That I Don't Have, Because I Traded in Cryptos. Am I f*****?" reddit. Accessed June 4, 2020. https://www.reddit.com/r/personalfinance/comments/84huks/i_just_discovered_that_i_owe_the_irs_50k_that_i.

•Trump, Donald J. "I Am Not a Fan of Bitcoin and Other Cryptocurrencies, Which Are Not Money, and Whose Value Is Highly Volatile and Based on Thin Air. Unregulated Crypto Assets Can Facilitate Unlawful Behavior, Including Drug Trade and Other Illegal Activity . . . ." Twitter. July 12, 2019. https://twitter.com/realDonaldTrump/status/1149472282584072192.

•US Regulators Target Bitcoin ATMs: 88 percent of the Funds Exit the Country via Machines NEWS | 19 hours ago Despite Russia's Confusing Crypto Laws. "US Presidential Candidate Andrew Yang Says Regulations Cannot Impede Crypto." Bitcoin News, February 1, 2020. https://news.Bitcoin.com/andrew-yang-crypto/.

•"What Is the Cryptocurrency Act 2020?" Yahoo! Finance. January 7, 2020. https://finance.yahoo.com/news/cryptocurrency-act-2020-180039429.html.

•"15 U.S. Code § 77b—Definitions; Promotion of Efficiency, Competition, and Capital Formation." Legal Information Institute. Legal Information Institute. Accessed February 7, 2020. https://www.law.cornell.edu/uscode/text/15/77b.

CHAPTER 14: INVESTING WITHIN YOURSELF

•Ayivor, Israelmore. *Michelangelo / Beethoven / Shakespeare: 15 Things Common to Great Achievers*, 2013.

•MWCM. "Principles of Success Part II: 'Don't Chase the Money'." MW Capital Management Pte Ltd., October 19, 2018. https://www.mwcmgroup.com/principles-of-success-part-ii-dont-chase-the-money/.

•Woetzel, Carter Lee. "CarterLWoetzel/Building-Confidence-in-Blockchain---Next-Steps." GitHub, June 6,2020. https://github.com/CarterLWoetzel/Building-Confidence-in-Blockchain---Next-Steps.