BRIAN KELLY

The Bitcoin Big Bang

How Alternative Currencies Are About to Change the World

WILEY

THE BITCOIN BIG BANG

THE BITCOIN BIG BANG

How Alternative Currencies Are About to Change the World

Brian Kelly

WILEY

Cover image: © iStock.com/pixelparticle
Cover design: Wiley

Copyright © 2015 by Brian Kelly. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

ISBN 9781118963661 (Hardcover)
ISBN 9781118963647 (ePDF)
ISBN 9781118963654 (ePub)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

For my wife, Dawn, this book is a testament to your unwavering faith in my stupid ideas.

Contents

Preface

Every so often I find myself with the insatiable desire to jump off a cliff and think about the consequences later. Some may call it curiosity, while others think I am just plain crazy. I typically relish the skepticism, as I have found that the best opportunities arise when everyone else thinks I am a little nuts. The Bitcoin Big Bang was one of these times—actually, truth be told, this time I was the one who was skeptical. Despite my fear, uncertainty, and doubt, I jumped anyway.

When I began writing *The Bitcoin Big Bang,* it was for selfish reasons: I had bought Bitcoin near the peak and now was in a losing trade and needed to know everything about this "investment." I figured I could turn my research into a book and learn a few things in the process. I did not know that I had stumbled on one of the most fascinating and promising technological advances since the Internet. When I first heard of Bitcoin, it was through the currency markets, and that is where my journey to Bitcoin Enlightenment began.

I mistakenly assumed that Bitcoin was an interesting new currency that had held little promise. After all, was the U.S. government really going to allow an unregulated currency based on computer code to replace the dollar? What I now realize is that the currency is

not the innovation; the blockchain technology is the game changer. The currency—bitcoin—is a fascinating alternative currency that has the potential to disrupt the global payment networks. However, it is the blockchain technology that is revolutionary.

The concept of the blockchain enables the transfer of secure information over an unsecured network. This may sound like a small step, but it is the first time in human history that this has been possible. The blockchain solves a multidecade-old problem in computer networking, and it can be applied to more than just currencies. It has the potential to end identity theft, create a secure Internet without the need for passwords, and revolutionize the way corporations do business.

When Jeff Bezos left a lucrative job as an investment banker to start an Internet bookstore called Amazon, everyone thought he was crazy. At that time, video stores like Blockbuster were in their prime and smartphones were landlines with an answering machine attached. Today, that same company (Amazon) is a leader in streaming video content to a handheld computer called a smartphone.

I do not know what alternative currencies will look like or accomplish over the next 20 years, but I do know that when a revolutionary technology is born, the world changes.

My goal with the book was to answer four questions:

1. What is Bitcoin, and why is it revolutionary?
2. How does it work?
3. Why are digital currencies a new type of investment?
4. How are alternative currencies going to change the world?

To this end, the book was written with two sections in mind. The first half of the book describes what Bitcoin is and how it works, while the second half illustrates the multiple uses of the blockchain technology and explores the ramifications for investments, business, and government.

An innovative technology was created by an anonymous programmer, who has given it away for free. This creation has spurred a technological explosion similar to the personal computer and the Internet, and, like its predecessors, alternative currencies are about the change the world.

—BK

Acknowledgments

When I began writing this book I thought it would be a solitary endeavor—countless hours writing alone to produce a manuscript that somebody might decide to read. Boy, was I wrong! This book would not exist without the contributions from friends and colleagues.

Let me start by thanking Jeffery Krames, who contacted me four years ago and convinced me I should write a book. It took a while, but this book is a testament to your persistence, patience, and conviction. You always knew I had a book in me.

To the CNBC *Fast Money* production team: thank you for supporting this project and for being an integral part of launching Nautiluscoin. Lisa Villalobos, the multitalented executive producer of *Fast Money*—you were able to take my slides of cryptographic hash functions and economic theory and turn them into a digestible television segment. You make it look easy. Michael Newberg, who was charged with producing a segment on a subject that I was still struggling to comprehend—you skillfully took an esoteric concept and turned it into a television segment that everyone could understand.

Melissa Lee, you were one of the first to understand the revolutionary nature of digital currencies. Your vision and intellectual curiosity are a big reason Nautiluscoin exists. Your ability to deftly juggle market-moving events and manage four traders with strong opinions is remarkable.

Which brings me to my *Fast Money* friends: Guy Adami, Karen Finerman, Steven Grasso, Jon and Pete Najarian, Dan Nathan, and Tim Seymour—you have all been an inspiration and I am constantly astonished at how fortunate I am to be able to work with you. You were all part of my journey to Bitcoin Enlightenment. You witnessed my skepticism, then my discovery, and along the way I may have convinced a few of you that there is something to this digital currency craze.

To my parents, who always encouraged me to be curious and embrace discovery—you made sure I always had opportunities to absorb, even in high school, when I thought I would never need to learn how to write.

I am forever grateful to the group at Austin Global Exchange: Justin Northcutt and Ryan Crow—you took a chance on a new currency and were true professionals throughout the entire project.

Nautiluscoin, as it stands today, would not exist without the talented coding skills of Jared Tate of DigiByte. I consider myself lucky to have met you before the world discovers your talent.

To the publishing team at Wiley, especially Lia Ottaviano—thank you for guiding this first-time author and answering an untold number of silly questions. To Evan Burton—thank you for believing in this project and being its champion.

Last, but certainly not least, to my wife Dawn, aka Mrs. BK—this entire project would not have occurred without your support. Besides listening to countless hours of my droning on about how amazing digital currencies are, you were a much needed sounding board. You always challenged my views—this book and I am better for it.

—BK

About the Author

Brian Kelly is founder of Brian Kelly Capital LLC, a global macro investment manager with a focus on currencies. He has 20 years' investment experience trading U.S. and international equities, foreign currency, options, futures, metals, and commodities. Throughout his career, Brian has specialized in trading multiple asset classes, cross-border investments, and risk arbitrage.

Brian is a CNBC contributor and can be seen on *Fast Money* (host: Melissa Lee), *Halftime Report* (host: Scott Wapner), and *The Kudlow Report* (host: Larry Kudlow).

Brian is a graduate of the University of Vermont, where he received a BS in finance. He also holds an MBA from Babson Graduate School of Business, with a concentration in finance and econometrics.

A passion for investments and entrepreneurship has led Brian to start several successful investment businesses. His most recent start-up (Brian Kelly Capital) is a global investment management firm specializing in global macro and currency investing.

Chapter 1

Bitcoin Is a Bubble

> When I see a bubble, I buy that bubble, because that is how I make money.
>
> —George Soros

Fad, scheme, scam, tulipmania, and *bubble* are all terms I have used to describe Bitcoin. The majority of my professional money management career has been spent in the currency markets, and as a so-called expert I was convinced Bitcoin was nothing more than a speculative bubble. It seemed impossible that a string of numbers backed by nothing and without an army could ever meet the accepted definition of a currency as a plausible medium of exchange, store of value, or unit of account. More than once, I confidently declared that Bitcoin was nothing more than "Tulipmania 2.0," a reference to the Dutch tulip bubble of the 1600s. Of course, the only thing I knew about Bitcoin was that people were calling it a digital currency, a term that was new to me. Unfortunately, not even ignorance could stop me from bellowing on national television that Bitcoin would not last.

I had first read about Bitcoin in 2011 while browsing my usual currency websites looking for investment ideas. In the late spring of 2011, the price of bitcoin had reached parity with the U.S. dollar, and by July, one bitcoin was worth $31. Any investment that has a 3,000 percent increase in value will attract a lot of attention, but two decades working on Wall Street has taught me not only to be skeptical but to automatically dismiss these investments as unsustainable bubbles.

Bitcoin appeared to be a quirky little project hallucinated by a cryptic computer programmer who was disillusioned with the post-financial-crisis world. It was interesting, but I did not think there was any money to be made, so I promptly forgot about this diversion and continued blissfully unaware that a revolution was under way. It was not until the autumn of 2013 that Bitcoin would reappear on my radar.

In October 2013, I was consumed with research on the end of quantitative easing by the U.S. Federal Reserve. The so-called taper had roiled financial markets, and I needed a template to guide my investment decisions. Since many believed that Bitcoin was a direct response to quantitative easing, the two concepts had become twinned, especially on the Internet. Through my research, I began to notice the price of bitcoin was once again on the rise. After stagnating below $31, the price of bitcoin had spent the past year climbing to $150.

As the price climbed, the media attention grew, particularly on the business channel CNBC, on which I appeared. If there is one thing I have learned from being on television, it is "if it bleeds, it leads," and Bitcoin was as close as business news gets to a bleeding headline. Not only was the price rising rapidly, but the clandestine creator made the story fascinating. Most importantly, people were interested. Perhaps we all sensed that something remarkable was happening and we all craved knowledge. Information becomes a valuable commodity during times of uncertainty.

Despite my deep skepticism, I was haunted by a quote from famed investor George Soros. Mr. Soros was talking about gold as the ultimate bubble when he was quoted by *The Australian* as saying, "When I see a bubble, I buy that bubble, because that's how I make money." Well, this was my bubble and it had been unknowingly stalking me for two years. I could no longer ignore the palpable euphoria. I wanted in—no, I *needed* in.

The Quest to Buy Bitcoin

In my day job, I am accustomed to taking risks, but as I contemplated buying into the Bitcoin hype, fear coursed through my veins. This was a different kind of risk; Bitcoin had a bad reputation. The notorious website Silk Road had just been shut down and its hoard of bitcoins seized by the FBI. Characters with monikers like Dread Pirate Roberts ruled this realm, while hackers constantly launched attacks. If I were to stride into this land flashing my Wall Street credentials, I would be an easy target. Caution and anonymity would be my friends on this quest.

Clicking on stealth mode, I typed "how to buy Bitcoin" and Google's algorithm churned out 166,000 results. The first page of results was meaningless to this neophyte, except for one: Mt. Gox. Since Mt. Gox was the largest exchange in the world, I was vaguely familiar with the name. It was comforting that Mt. Gox was the largest bitcoin exchange in the world, and I decided immediately to ascend Mt. Gox to make my purchase. Astonishingly, it did not bother me that only a short time ago Mt. Gox stood for Magic: The Gathering Online Exchange and was a place to trade magical game cards. Bitcoin was cutting edge, it was the Wild West; I needed to take a risk. In a spurt of rapture I convinced myself that since Mt. Gox was located in Japan and the inventor of Bitcoin went by the name Satoshi Nakamoto, then Japan must be the Bitcoin epicenter.

Doing my best impression of James Bond, I created a fictitious Gmail account to remain as nameless as everyone else who dealt in these "coins." My pulse quickened as I registered under my alias—I was unsure if I was breaking the law or stumbling upon a hidden fortune. I surveyed my new environs, and I decided to make a purchase; this was my first step toward untold riches. But it all came to a screeching halt when I realized that I overlooked one tiny detail—I needed an actual bank account with real money to buy the coins.

I was determined to cash in on my bubble and promptly formulated a plan.

When I signed into Mt. Gox, a message advised that there was a waiting list of people trying to buy bitcoins. The exchange was so busy that they could not process all the requests, and the message indicated it would be five days before my paperwork could be processed. I was

thrilled to have an additional five days to open a U.S. bank account for a "person" with only a fake Gmail address. It was not yet clear to me that my judgment had been compromised by visions of planes, autos, and jewelry. Finally, I drifted back to reality and began to hatch a better plan.

Even though Bitcoin was anonymous, I quickly recognized that my dreams of bitcoin billions required my personal information. I immediately began to look for a layer of security. Another Internet search led me to eBay, where sellers of bitcoins were plentiful. It appeared that I could use PayPal, which meant I did not need a bank account and my information would be safeguarded. Alas, I had once again overlooked a small, but important, detail. If I bought bitcoins on eBay, I would be a counterfeiter's dream. This is a currency that lives on the Internet. While I was accustomed to dealing in foreign currencies, buying Mexican pesos from JPMorgan is a long way from purchasing a digital currency from a stranger on EBay. I did not know if I should expect a zip file of computer code or an actual metal coin. Obviously, I needed Plan C.

After an appearance on *Fast Money*, where I disclosed parts of my Bitcoin buying adventure, a Twitter follower mentioned Coinbase as an alternative to Mt. Gox. I had not heard of Coinbase, so back to Google stealth mode I went. As it turns out, Coinbase is one of the largest digital wallets, and it is a bitcoin broker that could handle my purchase seamlessly. I felt even more comfortable when I learned that Coinbase was based in the United States and backed by one of the largest venture capital firms in Silicon Valley.

Now that I was back on my road to riches, I needed to register, verify a bank account, and wire funds. The entire process would take over a week: three days to verify the bank account, one day to buy the bitcoins, and another five days before the coins would show up in my account. This was unacceptable—I was about to make a fortune and every second counted. Sadly, I was out of options. Since I was technically inept and had absolutely no idea how Bitcoin worked, I was at a severe disadvantage. I just had to wait, which was a monumental task for this attention-challenged trader. For a week I checked my account like a child on the night before Christmas: Were they there yet? How about now? Now? Now? Now?

My anticipation was exceeded only by my excitement when the coins finally arrived. All that remained was relaxation, planning my private jet purchase, and waiting for the world to catch up and buy bitcoins. I was waiting for a greater fool than I, and it did not take long before a whole bunch of fools arrived. The price of bitcoin soared from my purchase at $795 to $1,200 in a matter of days. I quickly calculated the annual return—$400 in 4 days meant $100 a day; multiplied by 365 days meant I had just turned $795 into $36,500, a 4591 percent gain. This was going to be the greatest trade I ever made—drop the mic and walk off stage.

Not so fast, hero.

Within days, the Chinese government banned banks from dealing with bitcoins, effectively shutting down the largest market. The price plummeted to $500 almost overnight. There is a saying on Wall Street about losing positions: they start out as a trade and end up as investments—rationalization at its finest. My "can't miss, surefire" trade had just turned into an investment. I was in for the long haul.

Now that I was an "investor," I thought I better find out what I actually owned. Typically, I rely on a deep knowledge of the markets I trade before I place money at risk. In the case of Bitcoin, I had succumbed to the powerful emotion of greed. Ironically, I make a living seeking out greed and fear, acting only when other people's emotions have reached their zenith. In the case of Bitcoin, I was a rookie and I had paid the price of inexperience.

In order to supplant my ignorance with knowledge, I began to research Bitcoin as a currency. If Bitcoin was a new type of currency, then the logical place for me to start my journey was from a familiar point of view. Since Bitcoin was designed to have a finite money supply—only 21 million coins will ever exist—it appeared to be akin to digital gold. The process of mining fit with this analogy, and the fact that miners received free coins was intriguing. However, unlike gold, bitcoins were being used to purchase everything from pizza to Tesla automobiles. As a medium of exchange, bitcoins were fulfilling at least one of the three functions of money.

Like many other Bitcoin explorers, I had my "aha" moment when I realized that if people could buy a pizza with bitcoins as easily as a credit card, then Bitcoin was also a payment system. This disruptive technology

was a free payment system—no credit card fees for those who indulged in the pizza pie or the pizza shop. Not only was this technology disruptive but it was happening in my industry. I was hooked; I needed to know everything. It did not matter that by now I could sell my bitcoins for a small profit; I was in too deep to turn back.

Bitcoin Enlightenment

My path to Bitcoin Enlightenment careened between cryptographic hash functions and the simple balance sheet that is the beating heart of Bitcoin. Searching for the mysterious creator, Satoshi Nakamoto, made for interesting reading, but it wasn't until I looked at Bitcoin as smart money and a social network that I truly understood the revolution.

Removing the middleman has a long history of disruption in business—the personal computer placed mainframe computing power on the desktop, while the Internet enabled peer-to-peer communication. The collision of personal computers and the Internet spawned companies like Apple, Netflix, Twitter, and Facebook.

The Bitcoin Big Bang is a story of evolution. It is the evolution of currencies, payment systems, how money is used, financial services, and even the way business is organized. It is that moment when you realize the world has changed, permanently and forever. Evolution is a laborious grind, until BANG—everything changes at once.

Even though I knew Bitcoin was game changing, it was still in its infancy. If I became evangelistic about the technology, I risked appearing to be a kook who thought he saw a unicorn. Perhaps it was self-doubt or an innate longing to be part of a crowd, but I would be restless without validation. Then, seemingly out of nowhere, I stumbled on a series of quotes from venture capitalists who were committing big money to Bitcoin. My sanity was restored.

> Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.
>
> What technology am I talking about? Personal computers in 1975, the Internet in 1993, and—I believe—Bitcoin in 2014.
>
> —Marc Andreessen, inventor of the Web browser and cofounder of Netscape

Marc Andreessen is not only the inventor of the Web browser; he is also a founding partner of the venture capital firm Andreessen Horowitz, which has invested $50 million in Bitcoin-related companies, including my wallet service, Coinbase.

In 2010, *BusinessWeek* named Chris Dixon the top angel investor in the technology industry. In 2012, Mr. Dixon joined Andreessen Horowitz, and by 2013, he wrote these words:

> Like a lot of people I initially dismissed Bitcoin as a speculative bubble ("Internet tulip bulbs") or a place to stash money for people worried about inflation ("Internet gold"). At some point, I had an "aha!" moment and realized that Bitcoin was best understood as a new software protocol through which you could rebuild the payments industry in ways that are better and cheaper.

And Peter Thiel, the billionaire founder of another "little" payment system called PayPal, had this to say about Bitcoin:

> It is worth thinking about money as the bubble that never ends. There is this sort of potential that bitcoin could become this new phenomenon....

Mr. Thiel has gone on to invest millions in Bitcoin companies like BitPay. If you don't remember Peter Thiel from PayPal, you may remember his business partner, Elon Musk, the founder of Tesla. If that's not enough street cred, you may also recall from the movie *The Social Network* that Peter Thiel was one of the first outside investors in a promising start-up called The Facebook.

Twitter, Tumblr, Foursquare, Zynga, and Kickstarter are all companies in which Fred Wilson, cofounder of Union Square Ventures, was an early investor. What does he think about Bitcoin?

> We believe that bitcoin represents something fundamental and powerful, an open and distributed Internet peer to peer protocol for transferring purchasing power. It reminds us of SMTP, HTTP, RSS and BitTorrent in its architecture and openness.

These venture capitalists have made successful careers out of solving problems. If an idea does not solve a problem, it is unlikely the venture will be profitable. While I knew Bitcoin was important, I could not grasp the problem it was solving. Perhaps it was because I, too, had a

problem: my journey toward Bitcoin Enlightenment accidentally made me CNBC's resident expert, but I was struggling to define Bitcoin. I had a sense that something big was happening, but I could not put my finger on it. Maybe it was instincts honed by the sharp edges of financial markets or perhaps it was delusion, but I could feel the change. There is nothing like becoming a television expert to motivate your education. As an early Bitcoin "tourist," I knew more than most, but eventually that was not enough. The further I climbed the "expert" ladder, the more I found myself grasping for a definition.

Bitcoin is more than a medium of exchange; it is more than an emerging currency—and this technology has the revolutionary power of the personal computer and the Internet. I recoiled each time I read a dismissive article; they did not understand what I had seen … then again, neither did I. During this agonizing process, I stumbled on dozens of uses and a handful of interesting business ideas, but I found a simple definition elusive. Then, over an excruciating 48-hour period, I not only managed to annoy my wife, but also to distill Bitcoin to its four primary elements. Bitcoin was the fertile ground of a new currency; it was breathing new life into our antiquated payment systems; as smart money, it was creating new types of money flows; and it burned with the intensity of a social network.

Mainstream economists have hesitated to define Bitcoin as a currency because its price is too volatile to be considered a store of value and you cannot pay your taxes with bitcoins. There is no doubt the volatility is a huge hurdle; however, the price swings have become less pronounced as the currency has gained acceptance. As for taxes, you cannot pay the U.S. Treasury in Japanese yen or euros, either, but they are considered currencies. At the heart of the tax payment argument is an implicit assumption that the U.S. government is the ultimate enforcer of IOUs or money. In the later chapters, we will dive into Bitcoin's built-in IOU enforcement—no middleman or government needed.

Currencies Are a Matter of Trust

The question I constantly get is why anyone would accept a bitcoin in the first place. My answer is that, just like any other currency, it is a

matter of trust. One must believe that accepting this form of payment means they can use it elsewhere to purchase something they want or need. As long as you have a reasonable expectation that you will be able to convert a currency into a good or service, then "what" the currency is does not really matter. In primitive economic systems that used barter, currency did not exist, but people trusted that if they accepted a fur pelt, it could be used to obtain food and water.

Indeed, there have been crazier things than bitcoin used as currency. A seashell, specifically wampum, was once the currency of the land, Native Americans trusted that wampum could obtain goods and services. Wampum was difficult to obtain, since it lived offshore in the deepest parts of the coastline. However, the most important reason wampum became a currency was trust. When European traders arrived in North America, they immediately recognized the importance of wampum to the Native Americans, and they began trading with the currency. In fact, wampum was legal tender in New England from 1637 to 1661.

Wampum worked well as a currency as long as you were trading goods and services within Native America. However, outside of North America, wampum did not enjoy the same trust, and hence goods could not be purchased with the shells. Eventually, the British pound displaced the seashells, as traveling merchants needed the pound to obtain goods and services outside the wampum ecosystem. Those conducting business within the ecosystem were forced to convert their wampum into pounds, giving birth to the term *shelling out*.

Another way to think of this matter of trust is through airline frequent flier miles. Some of us use these miles to purchase reward tickets while others use them to upgrade to business class; in either case, these miles are currency. I am willing to hold a balance of miles in my account because I trust that I will be able to use them to purchase a service, a plane ticket. However, I cannot spend my United Airlines miles outside the ecosystem to buy an American Airlines ticket. In this way, wampum and frequent flier miles are similar; they work as a currency only within an ecosystem.

Much like Wampum and frequent flier miles, in the early days, bitcoin was closed ecosystem. As merchants began to accept bitcoin it took on the characteristics of a currency and more merchants meant a higher price for bitcoin. The value of bitcoin was joined with its growing user

base. In fact, many emerging currencies exhibit similar trends—unless it is accepted, it has no value. The first digital currency I created was called the BKoin; it sleeps in my computer and is not accepted anywhere. I tried to send some to my wife, but she barely cracked a smile—it is a dead currency.

Thinking of Bitcoin as a payment system is where most Bitcoin Evangelists have their aha moments. Unlike a credit card, where we are charged for the privilege of use and acceptance, making a payment with bitcoins is free and fast. Bitcoin does not require personal information, which should be welcome news to those who shopped at Target during the 2013 holiday season. The Bitcoin payment system has no national boundaries and no requirement for a bank account, making it the ideal technology for international money transfers and serving the underbanked.

Bitcoin was born out of the Great Recession and financial crisis of 2008. It was a reaction to the financial revolution that had occurred over the past 20 years. It gained traction as global central banks began to print money to combat the Great Recession. The early adopters felt that quantitative easing was a threat to their livelihood. But just like food co-ops led to the formation of wholesale clubs, so, too, will Bitcoin lead to more mainstream business adoption.

It took me several attempts to understand that Bitcoin's innovation was the removal of the financial services middleman. The biggest obstacles were the acronyms. In any industry, shorthand tends to confuse the beginner and aid the expert. My inexperience with cryptography, P2P networks, and open-source protocols meant I had a formidable task ahead. Remembering my dream of a private jet, I slogged through the language barrier toward my fortune, unaware that I would someday share this knowledge.

What Is Bitcoin?

One of the first things I learned was that Bitcoin was known as a peer-to-peer network, which is fancy computer-speak for no middleman. The concept behind the technology is as old as commerce itself: cut out the cost of a middleman and you can offer a product cheaper. Business

empires have been built on this concept, for example, the food co-ops of the 1970s in the United States were the first-generation Costco, BJ's Wholesale, and Sam's Club.

Peer-to-peer networks have a history of revolutionizing industries. Sean Parker's creation, Napster, is a great example of a peer-to-peer network that changed music. With Napster, music files could be shared among friends (peers) without having to go to Tower Records and purchasing the album. Once the album was purchased, your peer could make you a copy and walk it over to your house. This cumbersome exchange not only involved several middlemen; it also involved your getting off the couch. Napster cut out the middlemen and allowed you to share your favorite tune from the comfort of your home.

Of course, the middlemen were none too happy with Mr. Parker, and they launched a barrage of lawsuits to reclaim their turf. Eventually, the legal costs caused Napster to shutter, but not before it changed the music industry permanently. Many consider the single song file-sharing service to be a predecessor to Apple's iTunes. The recording industry was accustomed to selling entire albums chock-full of songs that few wanted to hear. What Napster did was illustrate that the consumer preferred à la carte music purchases, and Apple picked up on this demand. Napster may have changed how people shared music, but Apple changed how they purchased it. Even more, iTunes has changed the way music is recorded and released. Many may lament the death of the album, but Napster and iTunes have ensured that there is no turning back.

When thought of as a file-sharing service, Bitcoin it not too different than Napster. The files that are being shared are units of value rather than music. If you could find a grocery store that accepted music as payment for food, then Napster could become a currency like Bitcoin. Once again, it comes back to whether the file you receive (music or bitcoin) can be used to buy something else. As soon as the file can be traded for something else, it becomes a currency, and if by some miracle the rest of the world decides to accept music as payment, then the value of that "currency" will likely rise. Once something becomes a currency, a new level of security is needed.

The security of the Bitcoin technology is what makes it more suitable than Napster as a currency. At the heart of Bitcoin is a global ledger, or balance sheet, called the blockchain. This global ledger records every

transaction that takes place with bitcoin. From the moment a bitcoin is minted, its every move is recorded, and it is this record that ensures bitcoins cannot be counterfeited. In order to create the blockchain, approximately every 10 minutes the Bitcoin software compiles all the transactions that have occurred into a file called a block. This block contains a reference to the previous file and is a record of every transaction that has ever occurred. When all the blocks are linked together, it forms a chain of blocks, thus the blockchain.

The security of Bitcoin depends on the process of linking all the transactions. Imagine if a one dollar bill were tracked each time it was used, from its printing to eventual retirement. Every pack of gum, soda, flower, or toy that was ever bought with that dollar would be recorded. If a counterfeiter made a copy of this dollar bill, it would contain a record of the rightful owner, and when he attempted to spend it, the built-in security would disallow the transaction. A counterfeiter would have to go back and convince each merchant that the transaction never took place. In essence, a counterfeiter would have to change every single transaction prior to making the copy.

Bitcoin's solution to the counterfeit problem is the combination of the blockchain and miners. As more transactions are added, the blockchain makes it virtually impossible to change prior transactions. The miners are charged with confirming that the bitcoin being transferred is not counterfeit. The act of mining for bitcoins involves using powerful computers to solve a complex mathematical equation. The answer to the equation contains a key that verifies all the previous transactions. If this key does not match the previous transactions, then the miners know the bitcoin is counterfeit.

In very simple terms, this is how a bitcoin transaction works: If Keith wants to send a bitcoin to Alan, he must broadcast that message to the Bitcoin network. The miners listen for this message and then use supercharged computers to ensure that Keith is the rightful owner. Once they verify Keith's ownership, they allow the transaction to occur and record it in the blockchain. For their work, the miners are rewarded with free coins called a coinbase—currently, for every group of transactions (block) that a miner verifies, the miner receives 25 bitcoins.

As we continue our journey to Bitcoin Enlightenment, we will wrestle with several more terms that may challenge some and enthrall

others. For now, the most important terms to remember are *peer-to-peer network, blocks, blockchain,* and *miners.* The Bitcoin peer-to-peer network allows users to transfer value; these transactions are stored in files called blocks; these blocks are linked together to form a blockchain; and miners solve a mathematical equation that proves ownership of a bitcoin.

Is It a Currency?

As a currency trader and self-proclaimed economics nerd, I thought defining Bitcoin as a currency would be rather simple. In order for something to be called a currency, it has traditionally needed to be a medium of exchange, a store of value, and a unit of account. As a medium of exchange, Bitcoin passed with flying colors; when the first pizza was bought with bitcoin, it satisfied this condition. As a store of value, it fell a little short—wild price swings have made it difficult for Bitcoin to become a trusted store of value. Finally, as for a unit of account, the jury is still out. Currently, there are not any products or commodities that have their value expressed in units of Bitcoin, but this is changing rapidly.

Perhaps we are too tethered to the conventional definition of a currency as a medium of exchange, a store of value, and a unit of account. Ultimately, both paper money and bitcoin are only valuable as a currency if acceptance is widespread *or* required. It's the "required" condition that carries all the weight. If you don't pay your taxes, the government has the right to seize your property. We have given the government both the right to issue currency and the right to enforce its use; this is not a political statement—it's just the law of the land. The argument against bitcoin as a currency is that you cannot use it to pay taxes, and it is not backed by an enforcement authority like an army. Both of these are true, but the argument misses a bigger opportunity.

What if Bitcoin did not need to live up to the textbook definition of a currency—what if it were a hybrid? Maybe it's a commodity or maybe it's a payment system, or perhaps it is something in between. But bitcoin is being used as a medium of exchange, and regardless of its formal definition, the technology is revolutionary. Like many others, my aha moment came when I started thinking about Bitcoin as a payment system. Viewing Bitcoin as more than a currency allowed me to see that

it has all the hallmarks of a revolutionary technology—it is strong, fast, and efficient.

Bitcoin's strength is the lack of a single point of failure. When hackers attacked Target, they had it easy. All they had to do was find an open door into the single database that contained all the customers' personal information. Bitcoin does not require personal information, and the database is distributed across an infinite number of computers. While hackers have been able to find a way into some computers, none of the attacks hobbled the entire organization. Even the failure of Mt. Gox, formerly the largest bitcoin exchange, hardly caused a hiccup. Imagine if a major stock exchange closed without warning—our financial system would be in shambles.

Bitcoin is fast because it reinvents the middleman. Think about what it takes to transfer money from one person to another. First, we both have to open a bank account, which is accompanied by a mountain of paperwork to verify identities. Then I need to instruct my bank to withdraw money from my account by writing a check, sending a wire, or using an electronic debit. Once it arrives, the payment needs to be verified, cleared, and delivered. All along the way, numerous points of friction exist, and all along the way, this friction costs us a fee.

Bitcoin is efficient because the middleman is compensated by the technology. The Bitcoin software pays the middleman, also known as miners, a predetermined amount of money. Paying the miners bitcoins is also the channel by which the money supply steadily develops. The miners compete to be the first to solve a mathematical equation, which processes the transaction and ensures that the bitcoins are not counterfeit. The first to solve the problem receives freshly minted bitcoins. It is this innovation that makes it impractical to strip the currency from the technology. The currency is an integral part, similar to how without the "@" sign, e-mail would not work.

Arguing about whether it is a currency misses the point of the technology. Bitcoin is a tool that securely verifies, clears, and conveys financial transactions. In short, it redefines the role of the middleman in the financial services industry. E-mail enabled us to send a better message, faster and more efficiently. Bitcoin does the same thing for money.

Let's take a deeper dive into how Bitcoin acts as a tool to verify, clear, and convey financial transactions. The revolution is the combination

of the blockchain and the miners—together, these components become the reinvented financial intermediary. The blockchain records every transaction, while the miners verify and convey the transaction.

Starting with the very first bitcoin created, the Bitcoin software began recording its every move. I always find it easier to humanize new concepts, so let's call the first bitcoin a socialite named Genesis. Wherever Genesis goes, the blockchain records her movements. In essence, it is taking pictures of her every move and recording it for posterity. Every 10 minutes, these pictures are gathered into a file called a block. Inside this file is a picture of not just Genesis, but all her friends, too; wherever they went in the last 10 minutes is recorded in the file. Also included in this new file is a picture of the previous block. This picture of the past links all the blocks together, forming a chain called the blockchain. Have you ever taken a picture of yourself in a double mirror? The same effect occurs with Bitcoin: it appears you can see forever.

The blockchain is the paparazzi of the Bitcoin world. Wherever Genesis goes, she is followed by photographers: if she buys a pack of gum, the paparazzi are there; if she goes out to a club, the paparazzi are there; even if she just sits at home on her couch, the paparazzi are there recording everything. Now when Genesis gets spent at the club for a bottle of Crystal, the miners get involved.

The miners solve a mathematical puzzle that lets them see all the pictures the paparazzi took of Genesis. The miners go back and trace her every move to make sure the Genesis at the club is the real Genesis and not an imposter. The first miner to solve the puzzle and look at all the pictures is paid in bitcoins.

What makes Bitcoin strong is that anyone can be a paparazzo and anyone can be a miner. Anyone who downloads the Bitcoin software also downloads the entire blockchain, which means all the pictures are not stored in a single place. The pictures are distributed all over the world on an infinite number of computers. If one computer crashes, the Bitcoin network keeps humming along. If I spill coffee on my computer or I get hacked, the Bitcoin network just uses the other computers.

Think about what happened with Mt. Gox. This was the largest bitcoin exchange in the world. It was the New York Stock Exchange (NYSE) and Nasdaq combined—and it failed. Yet its failure did not cripple Bitcoin. There was a decline in the price of bitcoins, but the

network kept going, transactions were still processed, and the paparazzi kept following Genesis. Imagine if both the NYSE and Nasdaq shut down without warning. The financial system would seize, and we would probably have to declare a bank holiday to quell the panic. Yet after the failure of Mt. Gox, the amount of merchants accepting bitcoin is expanding and the ecosystem is growing.

The reason Mt. Gox hardly caused a hiccup is that the system is self-sustaining. From Iceland to Oregon, miners are competing to be the first to solve the mathematical equation, and if they win, the reward is 25 bitcoins or about $11,250. Eleven grand every 10 minutes is not a bad payday. In fact, there is a mining operation in Washington State that makes $8 million per month!

Obviously, the financial incentive has attracted an abundance of miners, just like gold did in 1849. And just like gold, as the price of bitcoin rises, the miners make more money. To give you an idea of how much computing power is chasing after that 25 bitcoins, as of today the miners calculate roughly 50 quadrillion mathematical equations per second. Yes, 50 quadrillion!

What is incredible is that all this computing power and the growth in transactions have happened organically. The Bitcoin network is not just alive, it is thriving! And it is all because of the self-sustaining mechanism at the heart of the system. The miner-blockchain interaction is sustained by the system itself. It is self-reinforcing. The self-sustaining, self-reinforcing process at Bitcoin's core ensures its survival.

So who sold the first coins and where did they come from? Many of the coins that were sold came from the miners—they are the coins received as a reward for solving the equation. This is how the miners turn their bitcoins into fiat currency.

Now what if these coins were premined and used to raise capital for any number of projects. How would this work? The creator of the coin mines coins before they are released. Remember, the paparazzi or the blockchain is always recording the action, even if the coin does nothing. Once the coin creator has a hoard of coins, she can sell them to the general public. The proceeds could be used for charitable donations, or they could be used to start a new business.

Another interesting part of the Bitcoin technology is that I can program a dividend into any transaction. For example, let's suppose I sell

you 10 percent of my company for 100 bitcoins. I can program into that transaction that for every dollar I receive selling my product, you automatically get $0.10. In this way, Bitcoin could be used as venture financing.

There is also another way to use Bitcoin to efficiently solve everyday problems. The next generation of Bitcoin involves Smart Contracts, which allow you to designate a bitcoin for a specific use. For example, if I agree to pay you a certain sum at a house closing, then instead of putting the money in an escrow account you can use Mastercoin to designate a certain number of bitcoins to be paid at a specified time. This is one way in which Bitcoin removes the middleman from escrow transactions.

Of course, with any agreement you will need a contract, but without a central authority, it becomes impossible to enforce—unless it is a Smart Contract, that is, a contract attached to a bitcoin transaction and stored on the blockchain. Contracts can be written directly on a bitcoin transaction specifying the use, timing, and parties in the transaction. All this information is "photographed" by the paparazzi (the blockchain) and enforced through the mining verification process. The miners do not opine on the contract; they just verify that both parties agreed and process the transaction. The blockchain becomes the decentralized, trustless enforcer of the contract.

It's Revolutionary

As I thought about the evolution of Bitcoin, it became clear that it is more than just a way to buy something cheaply and anonymously. Within the Bitcoin software are timestamps that allow you to schedule payments. Using this feature, payment terms on contracts and invoices can be programmed into the money, making it "smart." The smart money features of Bitcoin can even be used to eliminate trust banks when transferring generational wealth.

If you thought defining Bitcoin as currency was controversial, then calling it a social network is probably the straw that will break the camel's back, but stick with me. Twitter and Facebook are simply messaging systems—when I tweet a vacation photo and it is retweeted, that picture is given value; more re-tweets or "likes" implies a higher value.

In essence, I am submitting my picture to a network for verification. If the network agrees that this message has value, then it is "allowed" to be transferred. The exact same concept occurs with Bitcoin—at its core it is a messaging system—but since we are dealing with money, a higher level of security is needed. The Bitcoin network not only verifies that I own the vacation pic (no hacked accounts here), but I can also attach a value to my picture. If one of my followers likes the photo, it implies they agree with the value I have placed on my photo. The Bitcoin social network then records this agreement on value and allows me to use it elsewhere.

In the following pages, we will travel together to explore how the technology works and who invented it. This journey will take us into the Bitcoin mines and out into the ecosystem. We will learn why banks are so afraid and retailers are rejoicing. We will even create our own coin to answer some of the critics of Bitcoin. Finally, we will end in the land of Decentralized Autonomous Organizations and discover why these creations may one day compete with Fortune 500 companies.

Join me, if you will, on the path to Bitcoin Enlightenment. If you choose this path, I can't promise a campfire and a round of "Kumbaya" at the end, but I can promise that you will have a front-row seat to what could be the most disruptive technology since the Internet and the personal computer.

Chapter 2

Understanding the Digital Gold Rush

> You have to learn the rules of the game. And then you have to play better than anyone else.
>
> —Albert Einstein

In January 1848, James Marshall, a foreman working at John Sutter's timber mill, found a piece of shiny metal in the tailrace. The shiny rock was poked, prodded, and pricked until they could determine that, lo and behold, it was gold! With this discovery the California gold rush began. Within three years, San Francisco went from an outpost of 200 residents to a boomtown of 36,000. Few knew it at the time, but American icons were being born; Levi Strauss and Wells Fargo are the most recognizable, but don't forget Studebaker and even the modern-day name of the city's football team.

The discovery of gold resulted in a rush to mine because gold was the metallic foundation of the U.S. dollar. It has not always been

enough to back the U.S. dollar with the full faith and credit of the U.S. government. In 1848, the United States was in the childhood of its growth to superpower; it was not clear that the full faith and credit would be around in the future. Of course, the United States was not the first country to adopt the gold standard. The shiny metal has a 5,000-year history as a medium of exchange. But why? After all, gold is nothing more than a rock—but it's a special rock.

Gold has one unique quality that makes it popular as a currency: density. Gold is one of the most dense naturally occurring elements, and in fact it is more dense than iron. Its density makes gold an ideal medium of exchange. One ounce of gold can be carried easily and packs a lot of value into a small package. Suppose you were making the long cross-country journey. Carrying a trunk full of cash was impractical, especially if you were making the trip by foot. However, carrying an ounce of gold was not only lighter but much more secure, as it could be hidden in your clothing. A trunk full of cash is much more difficult to hide under your shirt.

As the financial system grew, gold continued to play a central role in the monetary system. In fact, it was not until 1973 that the United States completely abandoned the gold standard. The electronic age of finance made the property that made gold desirable irrelevant in modern financial transactions. Today, money moves around the world with the swipe of a finger and the click of a mouse. Don't be fooled—the fact that modern technology has allowed for the smooth transfer of money does not mean it is frictionless. All along the way money must pass through banks, credit card companies, governments, and central banks. Each of these players in the financial system represents a point of friction, and in finance, friction is synonymous with fees. While money moves around the world, it does not do so without the middleman.

This dynamic of a fee-based financial system consisting of a web of middlemen is being challenged by the invention of Satoshi Nakamoto. Even though we are still not sure if Satoshi is an individual or a group, the invention is rapidly disrupting finance. Bitcoin is quickly finding a way to disintermediate the financial services industry; that is to say, Satoshi Nakamoto was intent on cutting out the large middlemen in the centralized financial system.

There is more to the story of Satoshi Nakamoto and a decentralized financial system, but before we can jump down that rabbit hole we need to know the basics. Until 2013, when the price of a bitcoin soared from $10 to over $1,000, the cryptocurrency lived in the realm of coding enthusiasts and criminals. The technology was tainted by black market uses and lack of mainstream acceptance. In addition to the nefarious reputation, the speculative activity earned Bitcoin the label of Ponzi scheme and Tulipmania 2.0. What was lost in the cacophony was the technology that lay at the core: the ability to transfer wealth to anyone, anywhere—instantaneously, securely, and without a trusted middleman.

As Bitcoin gained mainstream attention, the rush to profit from the technology began in earnest. Bitcoin currency exchanges sprang up to facilitate the purchase of bitcoins, while digital wallet companies offered to securely store newly purchased coins. These exchanges and wallets are the beginning of the Bitcoin financial ecosystem and are the vanguard of a decentralized financial system. This evolution is not any different than when the founders of American Express, Henry Wells and William Fargo, created Wells Fargo & Company to provide banking services to California in 1852. Like Wells and Fargo, modern-day digital currency entrepreneurs are filling a need. However, while Wells and Fargo sought to be the intermediary, Bitcoiners are trying to remove the middleman.

At the heart of Bitcoin is a self-reinforcing process that verifies and transfers value. This process is called mining, and it is the new banker of the financial system. Traditional bankers stand at the center of the financial system and ensure that money moves from one rightful owner to another. The Bitcoin miners do the same thing but without the need to employ thousands or erect skyscrapers.

The popularity and profitability of mining for bitcoins grew as the digital currency's price began to rise. Miners unlock newly minted bitcoins by solving complex math problems and verifying that a transaction has taken place. In the early days, all the way back in 2010, mining could be done on simple home computers, but as it became more profitable, miners moved up to supercharged computers. Of course, there are plenty of companies that are all too happy to supply this digital pickaxe.

The digital pickaxe has evolved from a simple computer in a spare bedroom to what is known as an ASIC miner. ASIC stands for application-specific integrated circuit and is specifically designed to be

the first to solve the mathematical equation at the core of the Bitcoin network. Companies like KNC Miner, BitFurry, and Butterfly Labs are all profiting from the digital gold rush. In fact, demand for the products has been so robust that some have run into problems filling the orders. Outraged miners waiting for the latest machine have called foul on the delays, but the real concern is keeping up with the most recent technological breakthrough. Since Bitcoin mining is both a competition and a game of chance, the miner with the fastest computer has the best odds of being the first to guess the correct solution.

Perhaps these new businesses will become the next Levi Strauss, which in 1850 used its knowledge of canvas tarp manufacturing to create sturdy pants used during 16 hours of hammering rocks. It is likely that somewhere in the Bitcoin ecosystem there is a modern-day John Studebaker, who, before building his eponymous automobile company, manufactured wheelbarrows for the prospectors.

During the California gold rush, more fortunes were made by the merchants than the miners. Levi Strauss, John Studebaker, and Henry Wells and William Fargo learned about the gold-mining industry and then provided much needed products. The distinguishing characteristic of these empire builders is that they adapted to an emerging industry. They surveyed the landscape and applied their skill set; in the process, they built American icons. If one of us is going to become the next Bitcoin billionaire, then we need to learn a few definitions and the language of Bitcoin.

The Language of Bitcoin

First, you may have noticed that sometimes Bitcoin is spelled with capital "B" and is singular, while other times it is all lowercase and plural, as in bitcoins. Because Bitcoin is both a currency and a technology, it is accepted practice to use an uppercase "B" when referring to the technology and lowercase when referring to the currency portion—bitcoins. Paraphrasing and blaspheming the Georgia Satellites, if you've got some change in your pocket going ching-a-ling-a-ling … they are bitcoins.

Once you have you have your bitcoins, then you need to know how the Bitcoin network processes a transaction. The three pillars on

which Bitcoin rests are the blockchain, private keys, and mining. The blockchain is the record of all transactions, private keys are the security system, and mining is the process of verifying transactions.

The Blockchain

The earliest known banking records date to 9000 BCE, when farmers would trade grain for cattle. The transactions were literally written in stone, and these tablets became the first public ledgers. At the heart of Bitcoin is also a public ledger that stores every transaction that has ever occurred. When people refer to bitcoin transactions as being transparent, this is what they are talking about.

For example, those shoes you bought with bitcoins so your spouse could not see the charge—yep, that transaction was recorded in the blockchain. Don't despair, while we all can see that someone bought the shoes, none of us can determine who it was, thanks to private keys. Your secret is still safe.

The reason the early bankers wrote transactions in stone was to prevent double spending. The ledgers recorded who owned the grain and who owned the cattle. In this way, they prevented an unscrupulous farmer from selling grain that he did not rightfully own. This worked well if all the transactions went through a single banker, but as commerce expanded there was a need for another layer of security. A farmer who purchased grain in village A needed to prove that he owned it before he sold it in village B. Regrettably, the earliest form of security was violence: If you stole the grain that you sold to the banker in village A, you would likely be visited by thick-necked men looking to inflict physical harm. Thankfully, today we have a branch of mathematics called cryptography, which allows us to create mathematical proofs that provide security. For some, solving complex mathematical equations may be tantamount to physical harm, but fear not, there is no math needed to use bitcoins.

If Alice sends bitcoins to Bob, the Bitcoin software wraps that transaction in a cryptographic hash function, that is, a complex mathematical problem. This cryptographic hash function turns the message "Alice sends one bitcoin to Bob" into an unreadable string of letters and numbers that can be decoded only by a computer guessing at the precise

combination of letters and numbers. The alphanumeric string is unique only to the Alice and Bob transaction; every other bitcoin transaction gets a completely different encryption. Once the code is cracked, the miner can verify that Alice is the rightful owner through her private key.

Public and Private Keys

Like some of us, bitcoins have a public persona and a private persona. The public persona is known as an address, while the private persona is called the private key. The address tells people where you live on the Bitcoin network so that they know where to transfer value. When Alice sends Bob one bitcoin, Bob must provide the address at which he wishes to receive the payment. In addition, Alice attaches an address to the bitcoin she wishes to send and then broadcasts to the miners this message: "Alice owns one bitcoin that lives at this address (insert bitcoin address). Alice wishes to send this bitcoin to Bob at this address (BTC address)."

While Alice publicly announces her intention, she must also privately send Bob the key that allows Bob to unlock the transaction and prove he is now the rightful owner. Just like our real homes, there is a private key to every bitcoin that proves the holder of the key is the rightful owner. On the Bitcoin network, a private key is a secret piece of data that is protected by a cryptographic signature that proves your right to spend bitcoins.

The combination of your Bitcoin address and your private key is called your public/private key pair. While the Bitcoin network can always see your address, it can never see your private key. The software problem that couples your address with your private key is known as a wallet, and the best way to think about this is a checkbook. On your checks are an account number, a routing number, and a check number. You fill in how much money will be withdrawn from your bank account and designate who is authorized to withdraw. Additionally, you sign the check to make it valid. Bitcoin works the exact same way.

Your wallet constitutes both your bank account and your checks; they are combined in one efficient electronic storage system similar to online banking. When you "write a check" on the Bitcoin network, you take bitcoins from your wallet and type in the amount of the "check." Your Bitcoin address that is publicly broadcast contains your account

number and your routing number. The Bitcoin software digitally signs your "check" with your private key and sends the transaction to the network for verification and transfer.

Once broadcast, the blockchain records the fact that bitcoins were transferred from Alice's wallet to Bob's wallet. The Bitcoin code then compiles the most recent transactions into a file called a block. Each block contains a reference to the previous block of transactions, thus forming a transaction "chain," and voila—we have created the blockchain.

The Role of Miners

Now that we have a block of transactions, we must make sure none of these bitcoins have been spent before, and this is where the miners come into play. The Bitcoin software code gathers up all the transactions (blocks) and broadcasts the transactions to any computer that is listening to the Bitcoin network. The computers that are listening to the network are known as miners.

Since I like ice cream, let's use an ice cream example. Suppose a teacher is trying to find out who secretly gave him an apple (the transaction), and let's also suppose there is a mathematical equation that will tell him exactly who owned the apple before it was transferred to him. The teacher calls his class in from recess and broadcasts to the network (the kids) the fact that someone has transferred an apple. He writes the mathematical equation on the board and asks his students to solve the problem. Since he called the kids in from recess, he needs to give them an incentive to solve the equation. If the kids solve the mathematical equation, they will receive one scoop of chocolate chip ice cream. Since the answer to the equation contains the private key, once the equation is solved the teacher will know who gave him the apple. Finally, to be sure that the solution is correct, the teacher stipulates that six kids must come up with the same answer and they must show their work.

The kids, desperate for their reward, begin to work furiously on the solution, burning a lot of energy in the process. Eventually, one of the children solves the problem, and she is allowed to share the solution with the rest of the class. Now the rest of the class can use the answer to work backwards and prove that the original equation would produce

this answer. The first kid to verify the answer gets ice cream. The Bitcoin network works the same way.

A transaction (apple) is broadcast to the network (class of kids, aka miners), and the miners work to solve the equation and verify that the previous owner of the apple (bitcoin) had to right to give it to the teacher. Once six miners verify the transaction, they get bitcoins (ice cream).

Right about now you are probably thinking, "What a neat little incentive system—why didn't I think of that?" Well, in many forms, we already have. The carrot-and-stick technique has been around for millennia; it's just that Satoshi Nakamoto figured out a way to securely use the carrot-and-stick technique over the Internet. It may seem funny that an unknown computer scientist developed a program that we all "trust" to transfer value. The system was designed to be trustless, and, as such, the creator has become immaterial. The fact that we don't "know" the creator doesn't mean we can't use the technology—after all, none of us know Thomas Edison, but we all use electricity. The spark that created Bitcoin was Satoshi's white paper, and, like Edison's discovery, the "grid" has expanded exponentially. The Bitcoin ecosystem now includes payment processors, miners, equipment manufacturers, exchanges, and financial services.

How Do I Buy Bitcoin?

Hopefully by now you are beginning to see how the Kool-Aid is made, realized it is not poison, and are thinking about taking a sip. You are ready to rush out, buy your first bitcoin, and cash in on the digital gold rush. Well, slow down, cowboy. In order to quench your insatiable thirst for bitcoins, you are going to have to complete a few steps. First of all, you need someplace to store your coins. In the Bitcoin world, where you store coins is known by that incredibly technical name … wallet.

Now, don't go dusting off the plastic coin purse you received when you opened your first bank account. Remember, a bitcoin is simply a string of numbers that identify a unique unit of currency. The type of wallet you will need for this journey is an electronic wallet, and these e-wallets come in two forms: software wallet and web wallet. There is

also something called a paper wallet, but we will learn about that when we talk cold and hot storage. For now, let's not put the cart before the horse.

The primary difference between the two types of wallets is where your coins are stored. In a software wallet, your bitcoins are stored on your hard drive. This means that whatever computer you download the software wallet on will now become your bitcoin vault. If the computer crashes, you lose all your coins, unless, of course, you backed up the wallet elsewhere. If you don't want to have a vault on your laptop, then you can opt for a web wallet, which uses the cloud and provides access to your coins anywhere you can connect to the Internet. Similar to online banking, with a web wallet you can see your balance anytime you connect to the Internet. Like a traditional bank, the provider of the web wallet is now in charge of keeping the vault safe from thieves. However, unlike a bank, these web wallets are not insured by the government—if your web wallet company is hacked, you will have little recourse.

Your choice of wallet will depend on two very important factors, security and ease of use. Software wallets tend to be a little clunky to use for the novice, but you can encrypt and back up your wallet to a thumb drive for safe keeping away from those meddling hackers. The downside to using a software wallet on your desktop is that it requires you to download the entire blockchain. Downloading the entire blockchain means downloading every transaction that has ever taken place with bitcoins. This not only can take up a lot of memory, but it can also take a few days.

The original Bitcoin software wallet is known as Bitcoin-QT. Actually, it's more than a wallet—it is the Bitcoin software, the wallet is simply a necessary feature. When you download Bitcoin-QT, you will also be downloading the entire blockchain, and you will have access to every transaction that has ever taken place with bitcoins. But wait, there's more. You will also have the ability to mine coins. Unfortunately, the days of using the simple built-in miner have long passed. Mining these days means specially built computers with enough fans to cool an elephant on the savannah.

Two of the most well-known web-based wallets are Coinbase and Blockchain.info, together these companies have over three million downloads of their wallets. These wallets are incredibly user friendly

and do not require downloading all the information about the Bitcoin blockchain. Even more, companies like Coinbase will also purchase bitcoins on your behalf. There is no doubt that security is always a concern, but even before the Mt. Gox meltdown, these web wallet services were attracting large venture capital investments, which allowed them to add many layers of security.

Regardless of which wallet you choose, it will need to be filled. Remember, the bank didn't fill your plastic coin purse; they expected you to do the heavy lifting. So now you need a way to fill up your wallet with bitcoins—and just like in real life, you can choose to make or buy. That is to say, you can mine for bitcoins, and if you are the first to solve the mathematical equation, then you will be rewarded with freshly minted bitcoins. In a subsequent chapter, we will explore bitcoin mining in depth—for now, just know that if you choose this route, your electric bill will almost certainly double and your significant other could force you to move out. Both of these statements are stunning but true. It happened to Emmanuel Abiodun—his wife forced him to move to Iceland!

Assuming you value your current residence and significant other more than bitcoins, you will probably want to buy your coins via an exchange or broker. In order to exchange fiat currency (dollars, euros, yen, etc.) for bitcoin, you will need a gateway into the bitcoin network. Someone on the network needs to be willing to part with their bitcoins in exchange for cold hard cash. You can go about this task yourself by calling everyone in the phonebook and hoping you not only find someone who holds bitcoins, but also wants to sell them. Alternatively, you can do what most sane people do and go to an exchange or enlist a broker.

Exchange versus Broker

When I first purchased bitcoins, I used Coinbase. It was relatively pain free—except for the anticipation. If you want to purchase bitcoins with fiat currency, you must link a bank account to Coinbase and wire money, which usually takes a few days to complete approval. Once the fiat currency is in your account, Coinbase will contact an exchange and purchase bitcoins on your behalf. In order to prevent fraud, Coinbase

requires you to wait for your bitcoins for several business days to make sure the transaction clears. If you want your coins sooner, you can link a credit card to your account as backup payment. Many of the Bitcoin exchanges act in a similar way; you wire fiat currency to the exchange, and then you can purchase bitcoins from the myriad of sellers.

There is a very good reason for these brokers and exchanges to make you wait for your bitcoins. Unlike a credit card transaction, bitcoin transactions are irreversible—once the bitcoin is sent, it is gone from your wallet forever. With credit card transactions, if you do not receive the product you ordered, you can always call Visa or American Express and request that the charge be reversed. This does not happen with bitcoins. The problem with allowing credit card purchases of bitcoins is that an unscrupulous individual may purchase bitcoins with a credit card and then claim he never received them. The credit card company has no way to prove that he did or did not receive them and could reverse the charge, leaving the seller out of bitcoins and fiat currency.

Bitcoin is in the very early stages of development; in fact, many of the core developers consider Bitcoin to still be an experiment. As with any new technology, the landscape is changing rapidly, and both good and bad actors can appear overnight. As the ecosystem evolves, the cream will rise to the top, but at this stage, due diligence is your best friend. Before you wire money to any exchange, broker, or individual seller of bitcoins, check them out. The Bitcoin community has a strong sense of self-policing, and many of the bad actors are called out on the Internet well before any problems occur. If you wouldn't give $10,000 to a stranger in a foreign country to hold, then don't wire it to them to buy bitcoins either. Okay, safety tip over.

We are now equipped with the basic knowledge that will enhance our journey to Bitcoin Big Shot. Our next step is to understand what established businesses are doing about Bitcoin. In this digital gold rush, some companies are embracing the technology, some are fearful, and others are trying to adapt. Levi Strauss had plans to open a tarp shop in downtown San Francisco, until he looked around and realized that rugged pants were in high demand. You can be sure there are plenty of Levi Strausses looking around the Bitcoin ecosystem and trying to adapt their skill sets.

Who "Gets" It?

Thought leaders, corporations, and venture capitalists understand the transformative nature of digital currencies as a payment system. Moreover, the blockchain technology represents a revolution in computer science that is being used to transform industries. The explosion of Bitcoin businesses and applications has caught the attention of retailers, like Overstock, who are rejoicing over the frictionless and free transfer of value. However, middlemen like Wells Fargo are correct to be curious about a technology that threatens their franchise. As a first step, on January 14, 2014, Wells Fargo gathered with virtual currency experts to "learn more" about this technology. When asked about the meeting, Wells Fargo spokesperson Mary Eshet said, "It's a new, evolving … currency … and since we have so much interest and invested in payment systems, we want to understand everything that's relevant about it."

Certainly, the credit card companies have the most to lose from the Bitcoin disruption, but some are beginning to embrace the technology. In June 2014, MasterCard filed a U.S. patent that would enable it to integrate bitcoins into its global shopping cart. The initial shock and perhaps fear is receding, and credit card companies are realizing that their strength is the size of their network, not the underlying medium exchange. Nonetheless, the ability to transfer money with few fees will almost certainly hurt the profit margins of companies like Visa, MasterCard, and American Express. Bitcoin has the ability to replace credit cards; whether it will or not is yet to be determined.

At the other end of the centralized network are companies like Overstock.com, which began accepting bitcoins on January 10, 2014. Patrick Byrne, CEO of Overstock, took to Twitter and announced the results:

> #Bitcoin's first full day on @overstock.com was a huge success: 840 orders, $130,000 in sales. Almost all new customers. #stunned
>
> —Patrick Byrne, @OverstockCEO

What Mr. Byrne does not mention is that the process of accepting bitcoins is just beginning to be streamlined. Overstock, like every

other company, needs to convert the bitcoins received into fiat currency (U.S. dollars, euros, pounds, etc.) to pay its suppliers and vendors. These companies rely on payment processors to complete this task. Prior to payment processors, companies accepting bitcoins would need to trade them for fiat currency at one of the exchanges and then wire the money to the corporate bank account. This changed when pioneers like BitPay entered the market and offered the service of converting bitcoins instantly into fiat. BitPay not only converts bitcoins; it also provides an easy software solution to accept bitcoins that also integrates with a company's accounting system.

In 2012, BitPay made headlines by signing up over 1,000 merchants to accept bitcoins, and as of the middle of 2014, that number has grown to 30,000 businesses and organizations. BitPay, like other payment processors, enables online merchants to accept bitcoins with the same ease as credit cards. The advantage that this company offers illustrates the disruptive power of Bitcoin as a payment system. On the company website is a handy calculator that determines how much money a merchant can save by using Bitcoin. A typical merchant who processes $100,000 of payments each month might pay $3,255 in credit card processing fees. The same merchant accepting bitcoins pays Bitpay only $300 to act as its bitcoin processing agent, resulting in almost a $3,000 per month savings. Said another way, this merchant could increase its profit margin by 3 percent by accepting bitcoins, or it could use the savings to lower the price of is merchandise, thereby creating a competitive advantage.

The Gold Rush Is Just Starting

The pioneers of the Bitcoin Big Bang are only the vanguard. There is an entire economic infrastructure to be built. In 1850s California, once the easily accessible gold was collected, the gold rush began to fade. However, its legacy is ever present—California is still known as the Golden State, and San Francisco is a hub of entrepreneurial discovery. Even the road signs for California state routes are in the shape of a miner's spade. Likewise, the digital gold rush is beginning to influence its environment. San Francisco is a hotbed of Bitcoin start-ups, and both New York and California are vying to be the digital currency capitals. Unlike the

short-lived California gold rush, the Bitcoin Big Bang has the potential to be so widespread that this gold rush should last for decades. To be sure, some of the early Bitcoin miners collected the easily accessible "gold," but there is much more to this technology than just digital gold.

Applications are being developed using Bitcoin's blockchain technology to disrupt the legal professional, financial markets, banking, and even voting. Bitcoin as a currency, or medium of exchange, is just the beginning. It is the vanilla ice cream within the hot fudge sundae. Layered on top of the technology will be applications that enable peer-to-peer lending to boom, legal documents to become digitized smart contracts, and voting to take place from your mobile phone.

Like the Internet, the potential uses of Bitcoin are endless, which means this digital gold rush is just getting started. There is still time to become the next Levi Strauss or Wells and Fargo. In order to fulfill our destiny, we need to know more about the genius behind the technology and how he/she/they solved a problem that has stumped the brightest minds for over 30 years. Finally, we need to know why the creator, Satoshi Nakamoto, decided to stay anonymous and remain a mystery.

Chapter 3

Bitcoin Is More than Digital Gold

> Every informed person needs to know about Bitcoin because it might be one of the world's most important developments.
>
> —Leon Louw, Nobel Peace Prize nominee

When I first discovered Bitcoin, I was firmly in the "Tulip-mania" camp. How could a string of numbers, backed by nothing, and without an army to enforce its use, constitute a currency? Well, I hope you are beginning to see what I eventually saw—Bitcoin is more than a currency, and it is much more than digital gold. It's a disruptive technology that smashes together crowdsourcing, cryptography, and economics to produce the ability to quickly, securely, and frictionlessly transfer virtually anything. It is a quantum leap in the peer-to-peer network phenomenon. Bitcoin is to value transfer what Napster was to music.

There is more to Bitcoin than just value transfer, but in the early days the centralized payment networks are the low-hanging fruit that is easy for Bitcoiners to pick. Most people come to Bitcoin just like me—first a skeptic, then a student, and finally a believer. The creation of Satoshi Nakamoto transcends digital gold and solves a problem that has stymied computer scientists for over 30 years. The Byzantine Generals' Problem has been the major hurdle for secure transmission of value over the unsecure Internet. Satoshi Nakamoto provided a solution to this problem and then he/she/they slipped quietly away.

The enigma that is Satoshi Nakamoto has driven many to collect circumstantial evidence and declare a discovery. Alas, none of the Satoshi searchers have been able to find the elusive figure, and even the original Bitcoin developers who corresponded with Satoshi have lost touch. The initial hoard of bitcoins Satoshi mined is worth millions and is thought to be unspent. Who is this clandestine genius, and why the secrecy?

Searching for Satoshi

March 14, 2008, began like any other trading day; I perused the morning news and formulated my plan of attack. The S&P 500 had fallen more than 15 percent since October 2013, and the U.S. economy had entered a recession, but few could have predicted what was about to occur. The previous evening, embattled brokerage firm Bear Stearns was hit with a liquidity crisis. The investment bank's customers and creditors demanded their money back, rendering the company insolvent. This was an old-fashioned run on the bank, and true to its function as the lender of last resort, the Federal Reserve needed to act. Investors rejoiced when the announcement was made that JPMorgan, with the help of the Fed, would loan Bear Stearns money for 28 days.

As the euphoria subsided, investors began to digest the news and bought up Bear Stearns stock. I was skeptical of the announcement. Something was bothering me—I could not understand how investors could justify buying the shares of an insolvent company. Markets rarely live in the realm of the rational; irrational exuberance and fear are the states where markets spend the most time. I began to buy put options

on Bear Stearns stock, which would be profitable once the irrational extreme had been met and the price of the stock began to fall. At first my bet was a loser; investors continued to believe that 28 days was all Bear Stearns needed to extricate itself from the worst credit crisis since the Great Depression. In my mind, I was not making the bet that Bear Stearns would fail, just that investors were too excited about the bailout. By the end of the day, the stock price had fallen to $30 per share and my bet was in the money. I decided to keep my bet open over the weekend, believing that irrational pessimism had yet to be reached. I had no idea what the next 48 hours would bring.

After a tumultuous weekend of negotiations, it was announced that Bear Stearns had failed, and JPMorgan bought the remaining assets at a price of $2 per share. I had inadvertently made one of the best trades of my career, but the victory was hollow. The collapse of Bear Stearns had cost people not only their jobs but also a big portion of their life savings. The rationale given by the Federal Reserve for allowing the collapse was that Bear Stearns was insolvent and it was best to let a strong player like JPMorgan help clean up the mess. The Federal Reserve thought it was acting under its mandate to ensure financial stability; however, within six months Lehman Brothers had failed and the global financial system was on the verge of extinction.

What occurred was the failure at the hub of the financial system. By their own admission, global central bankers were slow to understand the severity of the credit crisis that was developing. The failure of Lehman Brothers and subsequent bailout of AIG brought this fact into sharp focus. Ben Bernanke, the chair of the Federal Reserve, was an academic scholar with a specialty in the Great Depression, and he was determined not to repeat the mistakes of his predecessors. Along with Treasury Secretary Hank Paulson, he presented a plan to recapitalize the banking system; it was called the Troubled Asset Relief Program or TARP.

Just a fortnight after the U.S. Treasury announced it would use TARP to purchase stakes in the largest banks, a paper was published via the Cryptography Mailing List describing a peer-to-peer cashless transaction system. In the middle of a financial crisis the obscure paper only made a ripple within the cryptological community. Just like my Bear Stearns trade, few had any idea how big this would become. The paper

was authored by Satoshi Nakamoto. The feature "Bitcoin P2P E-Cash Paper" presents the original posting.

Bitcoin P2P E-Cash Paper

Satoshi Nakamoto, Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at: http://www.bitcoin.org/bitcoin.pdf

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.

Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed but proof that it came from the largest pool of CPU power.

> As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.
>
> Full paper at: www.bitcoin.org/bitcoin.pdf
>
> Satoshi Nakamoto

Prior to publishing this paper on a thing called Bitcoin, Satoshi was a relative unknown. In fact, it was unclear if Satoshi was a single person or a group. Satoshi did have a profile on the P2P Foundation website that described him as a 37-year-old Japanese male, but a thorough scanning of Satoshi Nakamoto's coding and posts led many to believe he/she/they were not Japanese at all. The early coders who worked on Bitcoin and interacted with Satoshi via e-mail described Satoshi as fluent in English and commonly used British English spelling.

After posting the paper, Satoshi worked on the Bitcoin project until April 2011 and then quietly slipped away.

The Search

The search for Satoshi's identity began with some of the Bitcoin forum users sifting through posts looking for anything that would reveal the true genius. When the initial examination of the postings yielded few clues, an active Bitcoin forum coder named Stefan Thomas graphed Satoshi's 500+ forum posts. Thomas found that there were almost no posts between the hours of 5 A.M. and 11 A.M. Greenwich Mean Time. The implication was that Satoshi was sleeping during these hours. Going further, many assumed Satoshi was a conventional sleeper and this meant that Satoshi Nakamoto resided in the Eastern or Central Time zones of North America or in the Caribbean.

The problem, of course, was that everyone assumed Satoshi Nakamoto was conventional. If Satoshi is/was a single individual, he/she

would not only need to be a skilled computer programmer, but also to be familiar with cryptography and to have an intimate understanding of economics. The word *cryptography* finds its roots in the Greek words for "hidden" and "secret." Modern-day cryptography relies heavily on mathematical theory and algorithms to encrypt communications. Excellence in any one of these fields would qualify the individual to be called extraordinary. Excellence in all three fields would be astonishing by any measure.

Despite the formidable odds against finding a skilled cryptographer (especially one that did not want to be found), the search continued. Those in hot pursuit turned to linguistics to tease out Satoshi's identity. Terms like *bloody hard* in postings made many think he/she/they originated or lived in Great Britain. Even more fascinating is that within the Bitcoin code is a tag relating to a January 2009 *Times of London* report on the bailout of British banks. These clues were discovered by Joshua Davis and published in an article for *The New Yorker.*

Armed with well-reasoned circumstantial evidence, Joshua Davis put together a short list of potential Satoshis. After all, there were only a few people in the world with the knowledge to create Bitcoin. The requisite coding and cryptographic skills ruled out most in the economics profession, and so Davis turned toward the clandestine world of cryptography.

Even though he was still a student at Trinity College in Dublin, Michael Clear was a 23-year-old star in the cryptography world when Joshua Davis confronted him at the Crypto 2011 conference in Santa Barbara. He fit the description of "Satoshi" perfectly; by all accounts, he was a brilliant coder and cryptologist, had worked in finance, and had coauthored a paper on peer-to-peer technology. His British citizenship added depth to the picture, but when Davis asked Michael Clear if he was Satoshi, he simply replied, "I am not Satoshi, but even if I was, I wouldn't tell you." As you can imagine, this answer did little to quell the speculation—if anything, it heightened the mystery. Finally, after a media maelstrom, Michael Clear told the *IrishCentral*, "I have always vehemently denied it (being Satoshi). I could never allow myself to be even remotely given credit for someone else's creativity and hard work." This seemed to do the trick, and the investigation moved on.

Joshua Davis wasn't the only one searching for Satoshi. At about the same time, Adam Penenberg was collecting his own circumstantial evidence. He presented his admittedly unscientific but compelling research in an article for *Fast Company* magazine. His first bit of detective work was to find an obscure line of text from the original Bitcoin paper written by Satoshi Nakamoto. He settled on the phrase "computationally impractical to reverse."

Penenberg expectantly plugged the phrase into Google search and a patent application was discovered with the same phrase. The patent was dated August 15, 2008, and was for a method to encrypt secrets between computers. He concluded that transferring value from one computer to another was nothing more than a shared secret. Further investigation led him to look up when the domain name BITCOIN.ORG was registered, and he discovered it was registered a mere 72 hours after the patent application was filed.

Perhaps this happy accident was no accident at all. Penenberg set out to find the three men listed on the application. Neal King, Vladimir Oksman, and Charles Bry are all listed on patent #20100042841. Each of these men had extensive backgrounds in computer coding and cryptology. And each of these men denied that they together or separately are Satoshi Nakamoto.

The search had reached yet another dead end. Whether intentional or not, Satoshi had left enough breadcrumbs to satisfy the curious but not enough to satiate the hungry. Perhaps these dead ends were all part of Satoshi's plan to remain anonymous, or perhaps the correct clues had yet to be discovered.

The next name on the list may indeed be the most fascinating in light of the implosion of the Mt. Gox exchange. Jed McCaleb dropped out of UC Berkeley and founded the Mt. Gox exchange. McCaleb certainly has the technical background to be the famed Satoshi; in fact, he not only founded the peer-to-peer file sharing network eDonkey in 2000, but he is also one of the founders of Ripple, an alternative cryptocurrency. When Jed sold the Mt. Gox exchange, he was quoted as saying the exchange was "cool and needed to exist," but he no longer found it "technically interesting." The similarity of this answer to a quote from Satoshi's final e-mail had many believing McCaleb and Satoshi were one

and the same. However, just like his predecessors, Jed McCaleb has also denied being Satoshi.

More recent additions to the list of suspects are Shinichi Mochizuki and Nick Szabo. Mochizuki is described as an eccentric genius who solved the ABC Conjecture, one of the most complex mathematical equations in the world. It is speculated that Mochizuki created Bitcoin in his spare time—as if solving complicated math problems wasn't taxing enough. He posted his solution to the ABC Conjecture on the Internet as opposed to the more traditional academic journals, and then … he walked away. He has refused to explain his solution to mathematicians and has denied that he is Satoshi. Eccentric, yes. Satoshi? We will never know.

Nick Szabo is not only a former George Washington University law school professor, but he is also a computer scientist known for coining the term *smart contracts*. We will learn a lot more about smart contracts in later chapters. For now, what you need to know about Nick Szabo is that he invented a decentralized digital currency called "bit gold" and that he has denied being Satoshi Nakamoto.

As the search for a carbon-based creator fell short, many began to speculate that perhaps a corporation or government agency was behind the cryptocurrency. Perhaps there was a secret team holed up at Google surreptitiously cranking out code and shepherding the movement. Still others suggested that the first letters of four large tech companies could be used to spell Satoshi Nakamoto: SAmsung, TOSHIba, NAKAmichi, and MOTOrola. Not to be left behind, the conspiracy theory crowd began to think that the NSA or CIA had created the currency to track spending habits.

On April 23, 2011, the account associated with Satoshi sent its final e-mail, which stated, "I've moved on to other things. It's in good hands with Gavin and everyone." With those simple cryptic words the creator of the most fascinating invention since the personal computer and the Internet disappeared into the same ether from which he/she/they emerged.

By the way, "Gavin" is Gavin Andresen, the chief scientist at the Bitcoin Foundation; he, too, has been named a possible suspect in the search for Satoshi. Alas, like the others in the chain, he has denied that he is the enigmatic creator.

It was Leah McGrath Goodman who made the biggest splash with her expose of Dorian S. Nakamoto for the relaunch of *Newsweek* magazine. When Goodman tracked Dorian S. Nakamoto to his modest home in Temple City, California, she was betting that the "S" stood for Satoshi. She was convinced the creator of Bitcoin was hiding in plain sight. While Leah McGrath Goodman had corresponded with Dorian via e-mail, when she asked about Bitcoin, the communications ceased. Determined to follow this lead, she showed up unannounced at Dorian Nakamoto's home, but her unexpected arrival prompted Dorian to call the local police. With the protection of the Temple City police, Dorian Nakamoto met Ms. Goodman at the end of his driveway. When asked about Bitcoin, Dorian S. Nakamoto reportedly said, "I am no longer involved in that and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection."

The police officers that were called to the home confirm Dorian's words. However, the Bitcoin community is in denial. The Bitcoin Foundation issued a statement written by Jeff Garzik on its official blog (see the feature "We Are All Bitcoin").

We Are All Bitcoin

Jeff Garzik, Bitcoin Core Dev Team, Guest Blogger, March 6, 2014

There is never a dull moment in Bitcoin. Today we have seen heightened media speculation on the identity of Satoshi Nakamoto. As of this writing, we have seen zero conclusive evidence that the identified person is the designer of Bitcoin. Those closest to the Bitcoin project, the informal team of core developers, have always been unaware of Nakamoto's true identity, as Nakamoto communicated purely through electronic means.

Still, it is a useful opportunity to review Nakamoto's identity and its relationship to the current project. Bitcoin's design is intentionally decentralized in many ways—certainly, the

(*Continued*)

blockchain operation and P2P network—but it is more than that. Bitcoin blockchain data is zero trust. Each full node on the P2P network validates 100 percent of the transaction history, trusting no central authority. Beyond the data, the Bitcoin software itself is open source and available for review by anyone. Anyone may fork the software, create a better version, and gain users.

Everyone who is involved in Bitcoin understands the strength of the design. The designer, operating under a presumed pseudonym, reinforced this. There was no need to know and trust Satoshi Nakamoto. The design stood by itself, open to inspection by all. Satoshi Nakamoto ultimately created a "language" of sorts with the bitcoin protocol. A network protocol, like Bitcoin, is nothing more than a common lingua franca enabling multiple parties to communicate usefully with each other. Much like other spoken languages around the world, the bitcoin protocol grows and changes as its users change, ultimately controlled by no one.

The Bitcoin project is decentralized. It has no leader by design. Each community member contributes and collaborates with others based on his or her own needs, choices, and free will. Bitcoin's reference implementation has a chief scientist, but ultimately leadership always rests in the hands of every bitcoin user. The Bitcoin Foundation is opening affiliate chapters around the world, and others are organizing their own Bitcoin groups in a decentralized fashion. The Bitcoin Foundation is a Bitcoin leader, but certainly not *the* Bitcoin leader.

Satoshi's identity may or may not be revealed in time. Based on current research from Sergio Lerner, Satoshi does not appear to have moved or spent any bitcoins. Satoshi is unlikely to be sitting on a beach in Tahiti, next to a multimillion-dollar mansion. Satoshi is unlikely to be prepared for determined, potentially violent thieves and curiosity seekers. Curiosity in Satoshi's identity is understandable, but please consider

responsible disclosure, and the danger such a revelation may generate.

The Bitcoin protocol would not exist without Satoshi, who is without question a brilliant designer. However, Bitcoin will endure well past Satoshi, as Bitcoin is everyone who uses it, not just one person.

Dorian Nakamoto is a model train enthusiast and had reportedly worked on several classified projects for corporations and the U.S. government, but his financial situation did not scream of a person worth over $500 million. He lives in a modest home with a Toyota Corolla parked in the driveway. The original hoard of bitcoins thought to belong to Satoshi Nakamoto remains unspent, and many speculate that Dorian Nakamoto may have lost the private keys. If Dorian Nakamoto is the creator of Bitcoin, there could be a simple explanation for his outward financial appearance—he is a skilled cryptographer. Perhaps appearing to be a pauper is simply a façade, or cryptographic hash function if you will. In the film *Goodfellas*, Jimmy Conway tells his co-conspirators to remain inconspicuous after the famed Lufthansa heist; perhaps Dorian Nakamoto is heeding that advice.

Or perhaps he is not the real Satoshi. Just days after the *Newsweek* story was published, Satoshi's account on the P2P Foundation's Ning page came to life. The simple message was, "I am not Dorian Nakamoto." The creator and operator of the page confirmed that the account used to post this message was the same account associated with the original posting of the Bitcoin paper. However, there is no way of telling whether the creator of the account is the "real" Satoshi or just another beard.

Since collecting circumstantial evidence is in vogue in the search for Satoshi, I will add one more piece to the puzzle. A U.K.-based gaming company called Mind Candy has created Perplex City, an online city where residents solve complex puzzles and ciphers. In 2007 the gaming company issued a challenge to the residents of Perplex City: find an individual with just their first name and picture. They posted this challenge on the website www.billion2one.org. The picture appears to

be a selfie of an Asian man standing in Alsace, France. The one clue given to players is the gentleman's first name: Satoshi. It would be pure genius for the creator of Bitcoin to usurp the name of the man in this game and use it to obfuscate his true identity. Of course, like every other Satoshi searcher, I have absolutely no evidence that this occurred, but it sure would add to the mystery.

Why Is Satoshi a Genius?

Those who interacted with Satoshi agree that the one thing the creator did not want was Bitcoin to be associated with any one individual. As a decentralized system it needed to remain about the software, not the creator. If indeed the blockchain was to become the new trusted third party, a single point of failure could not be present. Bitcoin needed to be a community, a group of people coming together to solve a task. What Satoshi Nakamoto had done was to solve the Byzantine Generals' Problem, and his elegant solution required consensus.

The Byzantine Generals' Problem was first proposed by computer scientists Leslie Lamport, Robert Shostak, and Marshall Pease in 1982. In essence, the Byzantine Generals' Problem is the problem of establishing trust among unrelated parties over a communication network that cannot be trusted.

The Internet has given access to information to anyone who connects to the network. This in itself is unprecedented in human history and has sparked numerous democratic revolutions. Never before has the mass population had access to the same information as the leaders. However, as we know all too well, since anyone can post information to the Internet, that information cannot always be trusted. Before Bitcoin, trusted information was centralized at third parties like respected media outlets and government agencies. Of course, these third parties represent a single point of failure and have been found to not always perform their duties. In fact, some of these third parties have used their position of power to manipulate information for their own benefit.

The Byzantine Generals' Problem has confounded computer scientists for over three decades, and until Bitcoin, many thought the problem

was unsolvable. Satoshi Nakamoto's solution, called the Bitcoin protocol, not only gives every user of the Internet a way to securely transfer information, it also ensures the information is legitimate. This is a breakthrough in computer science and human history that cannot be overstated. With Bitcoin, the old saying that "you can't trust everything you read on the Internet" is just that … an old saying.

Bitcoin was designed to be trustless. That is to say, the system does not require the users to trust each other. All the users need is access to the "pictures" taken by the paparazzi to verify where every single bitcoin has been. A trustless system cannot have a central figure; it would undermine the entire project. Bitcoin was born out of the financial crisis of 2008, a time when trust was a scarce commodity.

At the core of our financial system is a confidence that the currency we are exchanging will be accepted elsewhere. This confidence is a direct result of trusted third parties vouching for its value. Whether this currency is the U.S. dollar, Japanese yen, or even a mortgage-backed security, if the belief in third party deteriorates then the entire system fails. Bitcoin was the right solution at the right time. It offered a way to be confident about value without the need for a third party. Bitcoin stepped in where investment banks had failed.

The disaster of Bear Stearns and the collapse of Lehman Brothers showed that single points of failure can lead to a complete system failure. The Federal Reserve saved the system by acting as the centralized lender of last resort, but the Fed paid for these actions with a loss of credibility. Even the revered former Federal Reserve Chairman Paul Volcker said in a speech that the Fed had taken "actions that extend to the very edge of its lawful and implied powers." Bitcoin may be a response to this loss of credibility and whoever created it went to great lengths to remove any centralized third party.

Perhaps Satoshi knew all too well that a centralized system is only as strong as the belief in central authority to do the right thing. If the Bitcoin creator intended to spark a revolution, it could not be constructed on a single point. It is for this reason that we may never know the real Satoshi. A skilled cryptographer who does not want to be found has the ultimate advantage, and Satoshi has so far demonstrated that anonymity is paramount.

Bigger than Satoshi

We may never find Satoshi, and if we don't, the Bitcoin ecosystem can thrive; that is the beauty of the decentralized nature of the technology. Hopefully, the elegant self-sustaining solution to the Byzantine Generals' Problem is becoming clear to you. Perhaps your mind is exploding with ideas about how to apply this solution to a myriad of industries. You are not alone.

As we will see in later chapters, individuals are building decentralized stock exchanges based on the blockchain technology; while others have taken Satoshi's original currency and improved upon the code to create new currencies. These so-called alternative currencies are being used to bring water to those who need it and to reduce the costs merchants and consumers pay to exchange goods and services.

There is not a person alive today who "knows" Thomas Edison, but that does not stop us from using his invention to power cities and drive our economy. Searching, finding, and getting to know Satoshi Nakamoto makes for headlines that sell magazines, but it is irrelevant to the use and function of the creation. Just like electricity, Bitcoin has become bigger than the individual.

The search for Satoshi started as a quest to find one man, woman, or group, but in a larger sense it is a quest to rebuild the fractured financial system. Trust was destroyed by the financial crisis of 2008 and Satoshi found a way to rebuild. The trustless, decentralized system called Bitcoin is a technology that the new financial system can be built upon. In particular, the concept of the blockchain or "paparazzi" recording all transactions could have a transformative effect on how the financial system works.

Over 300 years ago, the first modern central banks were established in Sweden and England, and for the past three centuries the financial system was built on a centralized monetary authority. The idea of a decentralized financial system is something that may threaten those at the middle of the current system, but it should be looked at as an opportunity. If indeed a new decentralized system emerges, then a new infrastructure must be built.

There will be opportunities for new JPMorgans to arise. Somewhere in Silicon Valley there may be another Henry Wells or William Fargo

already working on the next American Express and Wells Fargo bank. It has been said that out of crisis comes opportunity, and no place is that more evident than the world of alternative currencies. The search for Satoshi should be more about finding these opportunities rather than finding the creator. Even if Satoshi is unmasked, it should have no impact on Bitcoin or the new financial system that is being formed around it. The search for Satoshi is a quest for a better, stronger financial system. Finding Satoshi should mean that we have learned from past mistakes and embraced new ideas. It should mean we are on the path of rebuilding.

On March 14, 2008, we were fortunate to have fast-acting leadership. The actions of the Federal Reserve and Treasury probably prevented a complete financial collapse. Unfortunately, it is still unclear what, if any, price we will have to pay. Will inflation finally rear its ugly head, or will the inequality gap lead to social unrest? Or maybe, just maybe, these brave leaders found a solution to a problem that has plagued central banks for 300 years. If they have, it means they have found the cure for recessions and financial panics. Alas, my faith in human behavior leads me to believe that the extremes of fear and greed are larger than a central bank. A central bank can act as a speed bump to slow the panic or quell the euphoria, but a cure remains elusive.

Satoshi's creation can be an elixir for our financial system. If we have learned anything from the financial crisis of 2008 it is that a single point of failure has the potential to destroy the entire system. Satoshi's legacy will be one solution to this problem. Bitcoin and the concept of the blockchain is an elegant way to reduce the single points of failure and decentralize the financial system. To be sure, all human creations are flawed and along the way we will discover Bitcoin's limitations. However, decentralization is a step in the right direction. In the words of Victor Hugo, "Nothing can stop an idea whose time has come."

Chapter 4

Byzantine Generals' Problem

> He who knows when he can fight and when he cannot, will be victorious.
>
> —Sun Tzu

Successful entrepreneurs are constantly surveying the landscape for problems to solve. Being the first to solve major societal problem can not only lead to substantial wealth accumulation, but it can make the entrepreneur more popular than she ever imagined. We need not look much further than Mark Zuckerberg and Facebook for a prime example; he was frustrated with the inability to communicate with fellow students and was stymied by an exclusionary culture. His solution was to create a communication platform that was open to all—well, open to all that had the aptitude to attend Harvard. His solution became known as the social network; he became a billionaire and had a major motion picture made about the development of Facebook.

It is a safe bet that Hollywood will eventually make a movie about Satoshi Nakamoto, even if they have to make it up. The Bitcoin creator has gone to great lengths to conceal his/her/their identity, which makes the story even more fascinating. However, the attention that both the creator and price rise has garnered masks the real reason why Bitcoin is a game changer. The problem that Bitcoin solved has eluded every computer scientist since its conception; it's called the Byzantine Generals' Problem.

The Byzantine Generals' Problem was first proposed by computer scientists Leslie Lamport, Robert Shostak, and Marshall Pease in 1982. The original problem was posed this way:

> We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.
>
> The generals must have an algorithm to guarantee that
>
> A. All loyal generals decide upon the same plan of action.
>
> The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do.
>
> The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore also want to insure that
>
> B. A small number of traitors cannot cause the loyal generals to adopt a bad plan.

However, this description is really just an extension of the Two Generals' Problem first proposed by. A. Akkoyunlu, K. Ekanadham, and R. V. Huber in 1975 in "Some Constraints and Trade-offs in the Design of Network Communications."

The Two Generals' Problem begins with two armies that want to attack a city and pillage the riches that lay within. The fortified city lies in a valley between the two hills and can be conquered only if both armies attack at the exact same time. The generals decide to communicate the time of attack once they have had a chance to survey the city and they

position their troops on opposite hills. Once the generals arrive on their respective hills, the only way to communicate is to send a messenger through the valley, which risks capture or a false message being sent. The two generals' problem is that they need to communicate the time of a synchronized attack by sending a messenger through the unsecure valley.

The metaphor helps to understand the problem that a network of computers can experience if valuable information is being passed between nodes. Each computer on the network is called a node and is synonymous with general. The only way for the computers to communicate is via an unsecure spider web of phone lines, fiber-optic cables, and even satellites, that is, the Internet. The Internet in the Two Generals' Problem is the valley through which the message must pass. Each node on the network needs a way to determine if the message it receives is legitimate. As the United States National Security Agency illustrated, messages sent over the Internet can be intercepted, and that is problematic when trying to send something of value.

The problem that must be solved is how to communicate the message of "let's attack at nine o'clock" so that both generals can agree to launch the offensive at a synchronized time. This may seem simple, but its complexity lies in its subtlety. Once the first general sends the messenger, he has no way to tell if the messenger made it through the valley. Additionally, the receiving general cannot be assured that the messenger that arrives at his camp is the official messenger. Remember passing through the valley means potential capture and traitorous tampering.

At first glance, one might conclude that the solution is to send multiple messengers, since it is unlikely that all the messengers will be captured, and therefore a few legitimate messages will make it through. However, one quickly realizes that regardless of how many messengers are sent, there is still no assurance that the messenger who arrives is carrying the correct message. Again you may think that as long as a majority of the messages received say, "Let's attack at nine o'clock," then a consensus could be reached. However, neither general can be assured that their message got through or that the majority of the messengers who arrive are not traitors.

Of course, each general could send a confirmation that the message was received. Unfortunately, you can see how the same conundrum arises. Neither general can be assured that the confirmation is valid, even

if we allow for an infinite number of messages. If either general hesitates due to the uncertainty, then the attack will fail. This has been the problem that computer scientists have faced since 1975; the authors of the original conjecture concluded that the Two Generals' Problem was impossible to solve. The computer science field accepted this conclusion as fact, until Satoshi Nakamoto took a crack at it.

When Leslie Lamport, Robert Shostak, and Marshall Pease proposed the Byzantine Generals' Problem (BGP) it was an extension of the Two Generals' Problem. By adding more generals, the problem becomes even more complex. Network computing, and more specifically the Internet, became a real-world laboratory where the BGP posed a real-world problem. The Internet is an unsecure network of computers; it is the valley through which all messages must be sent. When Alice sends an e-mail to Bob, it must pass through a treacherous valley and there is no assurance that the message received is the message that was sent. The simple solution to protecting an e-mail was to encrypt the message, but that still did not offer the security needed to transfer something of value. It is too easy for a bad actor to send a false message that is encrypted; just because the message is wrapped in Kevlar does not mean its contents are genuine.

If Alice and Bob are dealing only with scheduling a meeting that probably neither wants to attend, safeguarding valid transmission is less important. If the time of a scheduled meeting was tampered with during transmission, making Bob late, then Alice could simply call Bob and tell him to hustle into the conference room. However, what if that e-mail contained proprietary intellectual property, would you trust sending that in an e-mail? Or what if the message being sent contained all the transactions completed via credit card at a major retailer like Target? As we have seen, in the real world, the BGP can have devastating effects when something of value is transferred over an insecure network.

How Does Bitcoin Solve the BGP?

A solution to the BGP required several moving parts working in concert. The solution required a method to protect the contents of the message, a way to reduce the number of messages sent, a way to detect a false message, and some way to pay for it all. Bitcoin solves the BGP

by encrypting the message, imposing a cost to decode the message, providing a way to verify that the message was legitimately decoded, and providing an incentive to the honest generals.

When a message is generated, the Bitcoin code uses cryptography to transform a message of any size into 64 bits, this is known as the SHA-256 algorithm for Secure Hash Algorithm. Using this algorithm, a message that is two paragraphs long will be reduced to 64 random alphanumeric characters; a two-sentence message will also be transformed into a 64-bit string of letters and numbers. Once the message is transformed, it becomes unrecognizable and can be decoded only by solving a complex mathematical equation.

The actual equation that needs to be solved is less relevant than how hard it is to solve the problem. The effort exerted solving the problem is proof that you worked on the solution. The equation needs to be hard enough that the fastest and sharpest minds or machines take the same time to come up with an answer. A standardized amount of time is required to ensure that the difficulty of the problem is not too hard or too easy. An excessively hard problem will stall the network as the computers take a long time to solve it, while an easy problem risks network security.

The Bitcoin code specifies that the equation must take the fastest computer 10 minutes to solve, and every two weeks it adjusts the difficulty so that the average time to solve is 10 minutes. The computing power and energy needed to solve the math problem serves as a cost to sending a false message. Using the Bitcoin protocol, if a treacherous general wanted to send a false message, he would have to pay for a fast computer and the electricity required to operate it. If a general wanted to broadcast a false message without doing the work to solve the equation, the other generals could simply look at how much computing power the traitorous general expended. If there was little or no computing power used, then the generals could immediate assume the message was false.

In order for the generals to verify that a message was legitimately decoded, each general must show proof that it took him 10 minutes to solve the problem. The generals do this by looking at the total amount of computing power on the network. If the total network is taking 10 minutes to solve the mathematical problem, then the generals can assume the messages being broadcast have been decoded legitimately.

Further, Bitcoin requires that six generals confirm they received the same message. By requiring confirmation and proof that work was done to solve the equation, all the generals can be assured that the message broadcast is valid.

Finally, the Bitcoin protocol provides an incentive to honest generals for being the first to legitimately decode the message. The first general to solve the problem and broadcast the valid message to the network receives compensation in the form of a currency. As the value of the currency grows, the incentive to be an honest general will also grow. In this way, Bitcoin provides a self-reinforcing mechanism to reward honesty.

The currency of this solution is a called a bitcoin (lowercase b) and represents a known piece of legitimate information. This information is known to be true because the Bitcoin protocol traces its origin to verify its legitimacy. Every piece of information (bitcoins) on the network is recorded from its inception. It is not too different than having the paparazzi recording every movement of a celebrity's life starting with her birth. These "pictures" are stored on a general ledger for everyone to see, but the Bitcoin protocol ensures that changing the pictures would be statistically impossible and prohibitively costly.

Bitcoin uses the science of cryptology and a proof-of-work scheme to solve the BGP. The Byzantine generals cannot trust that the message they heard was the legitimate message—in simple terms, the message could be "attack" or "retreat." The Bitcoin protocol wraps the message in an incredibly difficult mathematical equation, and the solution to the problem is the valid message of "attack" or "retreat." An added layer of security is accomplished by the cryptographic equation itself. While the solution can be discovered, it cannot be reverse engineered. A traitor or a hacker cannot start with "attack" and discover the mathematical equation wrapped around the message. The undecoded transformed message is a mystery until the cryptographic hash is solved.

To solve the BGP, Bitcoin sends the message to all the generals simultaneously. When all the generals receive the message, they begin to work on solving the math problem. The first one to solve the problem broadcasts the answer to the other generals. Once the other generals solve the problem, they can verify that they received the same solution by comparing it to every other general's answer. The computational

power used to solve the problem is proof that the generals did indeed do the work to solve the problem, aka proof-of-work.

Treacherous generals can broadcast a false message, but when the other generals solve the problem, they will not get the same answer that the traitor broadcast. When 51 percent of the generals verify the same answer, the message is deemed to be true. It is similar to how scientific breakthroughs are presented to the community to be verified. For example, if one experiment in one lab produces a method for cold fusion, other scientists are invited to replicate the experiment. If a majority of the scientists can reproduce the results of the original experiment, then a new breakthrough is declared.

Each time the experiment is successfully replicated, it becomes more difficult for a hacker or disloyal scientist to go back and change the results of every experiment. This is how Bitcoin becomes stronger and more secure as it grows. Moreover, loyal generals are rewarded with currency for legitimately broadcasting the correct message; this aligns the incentives of the individual with the incentives of the group.

51 Percent Attack

Now this elegant solution does have a major flaw—the Bitcoin protocol assumes that the nefarious generals could never gain more than 51 percent of the computing power on the network. Bitcoin imposes a cost to sending false messages, but it also provides an incentive to solve the mathematical equation. Since Bitcoin relies on the consensus of the majority computing power, it is vulnerable to 51 percent of the network's falling under the control of a nefarious party.

To understand the 51 percent attack, let's suppose we have a group of 10 generals all using the Bitcoin protocol to decipher a message to "attack" or "retreat." In this case, 6 of the 10 generals would need to confirm that the message was legitimate by comparing the message they received to 5 other messages. As long as a total of 6 messages match, then the entire group of generals agrees to follow that message. The flaw is that it assumes that all the generals are working independently.

If the group of 10 includes 6 traitorous generals, then it is conceivable that 6 traitorous messages could be sent out and agreed upon.

However, the likelihood of this ever occurring randomly is quite small, but not negligible, especially when dealing with the transfer of something valuable.

Suppose 6 of the generals decided ahead of time to send a false message—if this were to occur, the system would fail. But why would they want to do this? Using the BGP, we shall go back to the original reason for attacking the city: if the generals are successful, they each will receive monetary compensation. It is assumed that the city to be attacked is filled with untold riches that will be split among the conquerors. Bitcoin ensures that the correct message is sent and received by providing bitcoins to the first honest general to solve the mathematical equation.

However, this system breaks down if the incentive to solve the equation becomes more valuable than the wealth a general would receive upon a successful attack. Additionally, if the incentive (bitcoins) is significantly more valuable than the computer power needed to solve the problem, then the structure changes.

For example, let us set the initial conditions so that it costs each general $1,000 to buy a computer to solve the equation. Further, suppose the electrical cost to run the computer is $100, for a total investment of $1,100. If the general receives $500 for solving the problem and $700 for attacking the city, then he makes a profit of $100 and has a monetary incentive to remain honest. However, if the money received from solving the problem and attacking the city drops below $1,100, the general is unlikely to participate. Remember that all the generals must participate for the attack to be successful.

But what if the value of the incentive to solve the equation climbed significantly, for example, to $20,000. In this case, the general would receive more for solving the equation than for attacking. This is why the Bitcoin algorithm requires action upon solving the problem. The two acts cannot be separated. But there is another problem: the incentive is high enough to encourage nefarious behavior.

Any general could buy six computers and run them for a total cost of $6,600. Since this general would be the only one able to confirm 6 messages, he could control the network. Moreover, he would also control the most computing power on the network and be in a position to continuously be the first general to solve the problem. In this case, the general would receive $20,000 for solving the problem, while spending

only $6,600 for computational power. The $13,400 profit would be a powerful incentive to be dishonest. In Bitcoin language, this is called a 51 percent attack.

It is possible for a dishonest individual or group to purchase enough computing power to control the entire network. The Bitcoin solution to the BGP breaks down if the cost of computing power is exceeded by the incentive received. This is not just a theoretical problem; it is occurring as these words are being written. The power of the computers used to solve the mathematical equation has been increasing at an exponential rate. This has resulted in some groups, known as mining pools, to have enough computing power to control the entire Bitcoin network.

An Elegant Solution

In simple terms, the Bitcoin solution to the BGP is to replace communication with computation. Since sending messages is virtually free, Bitcoin imposes a cost to send those messages. This cost reduces the number of messages sent and, combined with the incentive to solve the equation, ensures that honest generals send and receive the valid message. It is an elegant solution, but, as we have seen, not without flaws.

The BGP in its purest form still remains unsolved. Satoshi Nakamoto imposed brilliant constraints on the problem and developed a solution that worked within these constraints. The fact that the pure BGP remains unsolved does not diminish the real-world application of this solution. As long as the constraints are present, the solution works. In the real world, we can apply this solution to an unlimited number of situations. The Bitcoin solution can be applied any place that secure information needs to be sent over an unsecure line of communication. This accomplishment cannot be understated—it is simply revolutionary.

While the potential applications are unlimited, the most obvious industry for Bitcoin to disrupt is financial services. Because Bitcoin provides a way to securely transfer value, it has the ability to remove a wide swath of financial service middlemen. The current financial system relies on centralized institutions acting as the traffic cops and collecting a fee for this service. The Bitcoin solution to the BGP holds the potential

to revolutionize the financial services industry. It holds the potential to decentralize the system.

A decentralized financial system is something that has not been present in modern history. The seeds of a decentralized system are crowdsourcing and peer-to-peer micro-lending networks, but without security it has been impossible to scale up these networks. Individuals may be willing to lend a small amount of money to get a creative project off the ground, but crowdsourcing to build a new factory has heretofore been unimaginable. The Bitcoin solution to the BGP makes large-scale crowdsource funding feasible.

Prior to Bitcoin, large-scale crowdsource funding was the territory of the banking system. In essence, a bank is simply a middleman that gathers funds from a large group of people and securely transfers those funds to those who need them. The fee charged for this service is justified by the trusted third-party role played by the bank. Anyone can apply for funding, but only those the bank deems trustworthy are given funds. Solving the BGP means the decision about allocating funds is removed from the bank and placed back into the hands of the holders of the funds.

A decentralized financial system is a radical departure from our current structure, but change need not be feared. A decentralized financial system is more democratic and has the potential to fund projects that may have otherwise been overlooked. Disintermediation often liberates an industry and allows it to flourish.

Chapter 5

A Decentralized Financial System

> Change is the law of life. And those who look only to the past or present are certain to miss the future.
>
> —John F. Kennedy

The question that most people ask is why Bitcoin has become so popular. It rose from the ashes of the financial crisis of 2008 to become a legitimate player in the global financial system. But what's all the excitement about, and why have people embraced digital currencies in general? The euphoria stems from the realization that Bitcoin could be the vehicle that transforms the financial system from centralized to decentralized. Our modern system of money transfer may be ostensibly based on bits and bytes, but at its core is an outdated centralized network of middlemen.

Banking as we know it finds its roots in the agricultural loans made between grain merchants and traders who transported goods across

Assyria and Babylonia around 2000 BCE. Records of transactions and loans were made at temples and palaces. In fact, one of the earliest known writings, The Code of Hammurabi, refers to laws governing a form of banking. The legacy of this financial system may be hard to decipher in today's modern financial world, but one key element remains. Then and now, the financial system revolves around a central point. In Babylonia it was the temples, while today it is the global central banks.

Banks that resemble our modern financial system developed during the Renaissance period in Italy. In 1397, Giovanni Medici established the Medici Bank to serve the wealthy merchants and traders of Europe. The Medici family grew its empire and became one of the wealthiest families in Europe by improving on the general ledger system. The Medicis are credited with developing the double-entry bookkeeping system that anyone who has taken a class in accounting would recognize—and, if you are like me, loathe.

The double-entry bookkeeping system may have appeared to be a quantum leap, but once again these financial institutions relied on a central point of control. Merchants, traders, and consumers all were subject to the rules, regulations, and sometimes whims of those holding the purse strings. As banking families grew wealthy, it became even more difficult for the man on the street to open and operate a bank. Economies of scale and political power served as effective barriers to entry. Modern commercial banks owe their position at the center of the financial system to the legacy established by the Medicis and others.

During the Qing Dynasty (1644–1911), China used a bimetallic monetary system of copper coins and silver ingots. The square copper coins had a hole in the middle so they could be measured in strings. If a person with 100 loose coins wanted to transfer them to another, they needed to be in a string. This person could go to a money changer and exchange the coins for a string of 100; however, for his troubles, the money changer would keep a coin, returning a string of 99. This fee system resembles the bank charges we experience when wiring money between two parties.

On the other side of the world, the Bank of England was created in 1694. The Bank of England was a solution to a financial problem that the King of England was facing. After being defeated in war by France, King William III wanted to build a strong navy, but his finances were

in such a dire condition that he could not obtain a loan. The solution was the Bank of England—a newly created middleman.

The Bank of England underwrote a loan to King William, and subscribers to the loan were given shares in the Bank of England. This way, the creditors had equity in the Bank of England if the king defaulted on his payments. In order for the equity of the Bank of England to have value, it was granted the sole power to issue bank notes. Today, the Bank of England serves as the model for virtually every modern central bank.

Jump ahead 200 years to 1871, when Western Union completed the first money transfer via wire. These "money orders" were the first peer-to-peer (P2P) network. For the first time ever, a person in New York could instantaneously transfer money to somebody in San Francisco. At the time, this was revolutionary. Wells Fargo had built a veritable empire from the physical transfer of wealth via its stagecoaches, but now with the tap of a telegraph the stagecoaches became quaint relics. However, the transfers were possible only because of a centralized network of banks and telegraph lines. These represented friction, cost, and a single point of failure.

Western Union could not have existed if telegraph lines did not extend across the United States. Additionally, once the money order arrived at its destination, the Western Union office would need to withdraw cash from its bank—without the local Wells Fargo bank branch, this could not be accomplished. Similarly, Bitcoin could not exist without the Internet or the evolution of P2P computing. Like the Western Union money order, Bitcoin utilizes existing technology in a new and novel way to provide a service that makes value transfer easier and cheaper.

Our modern financial system may appear to be advanced, but at its core it is an inefficient centralized structure. Anyone wishing to transfer money or wealth to another individual must wade through a series of middlemen, all more than willing to charge a fee. Banks charge for holding your money, while credit card companies charge you to spend your money. Sending a wire domestically not only has a monetary cost, but also the cost of time lost. Driving to the bank, filling out a wire transfer form, and then waiting hours for the confirmation are all costs of sending money.

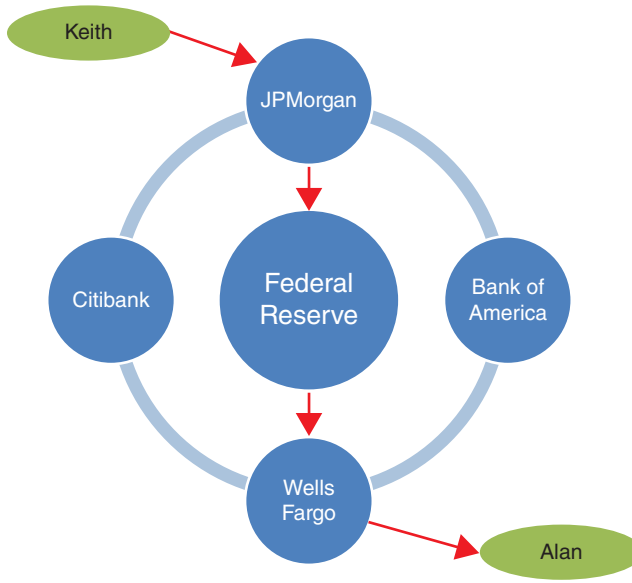

Figure 5.1 A Simple Transaction in a Centralized Financial System

A simple transfer of money may look something like this: Suppose Alan has performed landscaping working for Keith and is now requesting payment. Alan sends an invoice to Keith, who then must send payment via his bank account. In the simplest terms, if Keith wants to transfer money to Alan, he must contact his middleman (JPMorgan) to use the Federal Reserve wire system to send money to Alan's middleman (Wells Fargo), which sends it to Alan's account. Along the way, the banks create friction in the form of fees. See Figure 5.1.

This system is not too different from the ancient grain traders who would trek to the nearest temple to record a transfer of goods. Those wishing to finance a business during the Renaissance would likely need to contact the Medicis, who would either find a willing lender or make the loan themselves. The key, of course, was the hub-and-spoke system that we still have today. Those at the middle have an advantage, their position gives them power. Bitcoin changes all this.

The power concentration was a direct result of the inability to solve the Byzantine Generals' Problem. While this problem was formally

named and examined in 1982, it really has been around for millennia. Bankers have traditionally played the role of the trusted third party, stepping between unrelated actors and ensuring that the message transmitted is legitimate. Prior to Bitcoin, the only way to trust that the message was real was to enlist a neutral third party. When the message was a conveyance of value (aka money), the bankers emerged as the middlemen.

What if the power were not concentrated in the middle? What if every player in the financial system no longer needed a trusted third party? What would this financial system look like?

Grand De-Central Station

A financial system devoid of trusted middlemen would be a radical departure from the system that has been in place the better part of human history. However, that does not mean other systems have not existed; they were simply impractical to implement. The barter system was a primitive form of trade that had one major flaw. Economists call the flaw in the barter system the *coincidence of wants*. In a barter system, if you were a corn farmer and wanted a cow, you would need to find an owner of a cow who wanted corn. In a small community with a closed economy, this system was sufficient, but as trade flourished and economic systems opened up, a new way to exchange goods was needed. Money was created to solve the coincidence-of-wants problem.

With the advent of money the barter system vanished, but a new problem arose. How could a merchant trust that the currency being offered by an unknown buyer was legitimate? Merchants turned to newly invented trusted third parties called bankers. These bankers would stand in the middle of the transaction and verify its legitimacy. Bankers, like the Medicis, developed a ledger system that was designed to prevent double spending and counterfeit currencies. The middleman, or banker, had been the only way to solve the Byzantine Generals' Problem until Satoshi Nakamoto created Bitcoin.

Bitcoin is what is known as a decentralized distributed peer-to-peer network. This type of network allows people to transfer something of value without the expense of a middleman. Before the Western Union telegraph, the Pony Express was the only way to transfer information

across the United States. Similarly, prior to e-mail and the Internet, the U.S. Postal Service had a virtual monopoly on information transfer. Bitcoin is about to do to the financial services industry what the telegraph did to the Pony Express and e-mail did to the U.S. Postal Service.

Before we dive into the winners and losers from this disruption, it will be helpful to examine the three types of systems that exist. Computer scientists are well versed in the different types of systems that exist, but since financial services has operated only one way, there was no need to examine other ways to conduct transactions.

When describing the types of system, we will use the computer science terms and relate them to the financial system. These systems describe how a process works—that is to say, a process can have a single middleman, groups of middlemen, or operate directly peer to peer. See Figure 5.2.

The three most common types of systems are:

1. Centralized
2. Decentralized
3. Distributed

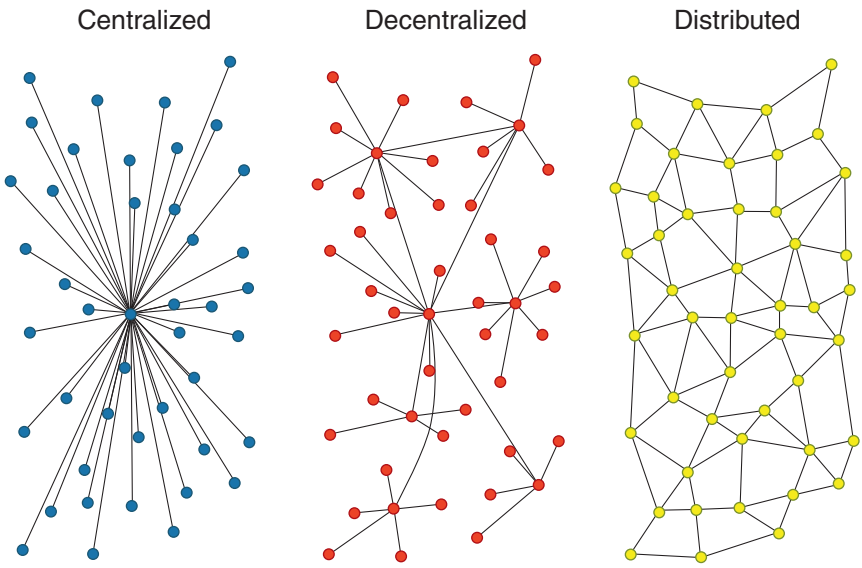

Figure 5.2 Types of Systems
SOURCE: p2pfoundation.net

A centralized system can best be thought of as a hub-and-spoke structure, where the key player sits in the middle and directs all the traffic. This is not just the structure of the modern financial system; it has also been used by commercial airlines and city planners. The city of Boston is nicknamed "The Hub" because the city lies at the center of a spoke system that makes up the suburbs. At rush hour, if an accident occurs at the center of "The Hub," it can impact commuters throughout the Greater Boston area. Moreover, anyone who has flown through Atlanta or Chicago during bad weather can also tell you about the flaw in the centralized system. A thunderstorm in Atlanta can easily cause delays in Los Angeles. In other words, if the hub fails, the spokes fail as well.

While a messy commute or delayed flight can be extremely frustrating, they typically are resolved with little effect on the future function of the system. Tomorrow, traffic will clear and the flight to Los Angeles may arrive early using the same centralized system. However, the financial crisis of 2008 shined a harsh light on the limits and dangers of a single point of failure in a financial system. A failure at the hub can mean that the system does not function tomorrow. By its own admission the Federal Reserve Board of Governors and its chairman, Ben Bernanke, did not recognize the severity of the financial crisis that was unfolding. Chairman Bernanke famously said that the subprime crisis was contained and would not threaten the rest of the economy. He was wrong and the financial system came to a halt. To his credit, when Chairman Bernanke recognized his mistake, he acted boldly and swiftly to prevent a complete financial collapse.

If Ben Bernanke, Hank Paulson, and Tim Geithner had not been able to resuscitate the centralized financial system, it is entirely possible that the global economy would have slipped into a depression worse than the 1930s Great Depression. The Great Depression is another example of the perils of a using a centralized financial system. The Federal Reserve not only failed to recognize the severity of the economic downturn; they may have exacerbated it by inaction. Further, the executive and legislative branches of the government also failed to prevent the crisis from spreading.

In a 1990s paper, "The Gold Standard, Deflation, and Financial Crisis in the Great Depression: An International Comparison," Ben Bernanke argued that the gold standard at the center of the financial

system shared the blame for creating a deeper economic malaise. Bernanke identified three flaws in the gold standard that contributed to the depression's becoming Great:

1. The asymmetry between surplus and deficit countries in the required monetary response to gold flows.
2. The pyramiding of reserves.
3. Insufficient powers of central banks.

Analyzing whether Bernanke was correct is beyond the scope of this book, but what is relevant is how a centralized system like the gold standard can suffer from failures at the hub. When Bernanke writes about the "asymmetry between surplus and deficit countries," he uses the example of France's refusing to play by the "rules of the game." For the international gold standard system to operate correctly, the countries that were experiencing gold inflows should have allowed their economies to inflate. While France was the recipient of gold, it did not allow the money supply to inflate, and Bernanke suggests this led to an exacerbation of the global downturn. If we think about the gold standard as a centralized system, we can see that the failure at the center caused the entire system to fail.

Pyramiding of reserves occurred when central banks would abandon foreign currencies that were being actively devalued. This reduction in reserves may have led to a reduction in global money supply. Bernanke also suggests that major European banks did not have the sufficient powers to conduct open-market monetary operations. Tomes have been written about the validity of these claims, but one fact remains: the institution at the center failed to act in a way that would benefit the entire system. It was this flaw that is more likely to blame for the extended period of economic depression.

A decentralized system seeks to correct the flaw by creating multiple hubs and spokes. In a decentralized system, there are many nodes (or hubs), each charged with ensuring the smooth flow of traffic, whether the traffic is information, text messages, or financial transactions. The Regional U.S. Federal Reserve System is a good example of a decentralized system. Each of the regional Federal Reserve Banks must make sure the financial plumbing in its region is working. However, the regional Federal Reserve Banks must report back and comply with the Federal

Reserve in Washington, D.C. This structure creates a single point of failure, that is, the Federal Reserve Board. If the Federal Reserve Board of Governors fails at conducting policy, then the entire system fails.

A decentralized system is superior to the centralized system when preventing a failure at the hub is essential. There remains a risk that multiple hubs fail at the same time, but it is a step forward in the evolution of systems. It is also particularly useful when each hub can act autonomously.

The next evolution is a distributed system, where every player acts as a hub. Each individual, business, computer, or government all have the same responsibility—ensure the smooth functioning of the system. In a distributed system, if one node (or hub) fails, the other nodes simply pick up the slack and make sure traffic flows smoothly. A distributed system works best when the decision-making process can be automated or coded into a series of yes/no questions. If each node is responsible for the same output then the decision-making process must be identical. Using the example of the "rules of the game" of the international gold standard mention by Ben Bernanke, France would not be able to prevent the money supply from inflating. France would simply act as one node in the financial system; if it decided not to inflate, then the other nodes would take over and inflate France's money supply. Immediately, one can see why this type of system has yet to be integrated into sovereign economies. Giving up control of the money supply is tantamount to giving up national sovereignty.

Examining the monetary system of Hong Kong, we can see where a conflict may arise if a distributed system is not designed properly. Since 1983, Hong Kong has pegged the foreign exchange rate of the Hong Kong dollar to the price of the U.S. dollar. In practice, what this means is that if the U.S. dollar is devalued, then the Hong Kong dollar will also fall in value and vice versa. Essentially, Hong Kong has outsourced its monetary policy to the U.S. Federal Reserve. This worked well when the U.S. Federal Reserve was not actively seeking to devalue the dollar.

The Hong Kong economy is now tied more closely with the Chinese economy than it was in 1983. The result is that the United States may be devaluing its currency to spur the U.S. domestic economy, while the Hong Kong economy is exposed to the growing Chinese economy. By outsourcing its monetary policy, Hong Kong risks stimulating its

economy at the exact moment it should be taking steps to slow growth. The result could be either rampant inflation or a break of the U.S. dollar peg. For our purposes, this is an example of a flaw in a distributed system; more accurately, the system must be designed to correctly handle these situations.

Since the Bitcoin economy is still growing, and it is doing so at a time of massive global economic integration it has an unprecedented opportunity to be the flexible solution to synchronizing monetary policy. If left alone, the Bitcoin economy has the ability to rapidly adjust to imbalances without relying on a central authority to make the correct decision. As a distributed system, each node in the Bitcoin network is charged with ensuring that financial transactions are genuine. Bitcoin accomplishes this task with 31,000 lines of code designed to trace every transaction back to its origin to confirm legitimacy. Because Bitcoin is a financial system, it uses cryptology to encrypt the transactions and keep them safe from would-be hackers.

Recall the transaction between Keith and Alan, where they needed to use the clumsy centralized web of middlemen to transfer value. Using the peer-to-peer, frictionless Bitcoin network, Keith can instantly transfer value to Alan for free. Figure 5.3 shows what that network looks like using Bitcoin.

Do not let the simplicity of the graphic fool you into believing that the Bitcoin network is not sophisticated. Bitcoin has done what no other computer program has done in the history of financial systems—it has automated the role of the middleman. Moreover, the developers of Bitcoin have given it away for free. The Medici family gained power and wealth by making a simple improvement to the existing system. Imagine if they had invented a new system altogether.

The revolutionary accomplishment of Satoshi Nakamoto was to reduce the complicated tangle of global financial middlemen into an elegant software package that can be downloaded onto a smartphone. This feat is not just astounding—it is unprecedented.

Figure 5.3 A Transaction Using the Decentralized Bitcoin Network

The history of business is replete with examples of industries that have been transformed beyond recognition by disintermediation. When was the last time you walked into a travel agent's office? Or asked a real estate agent for a brochure? Or looked in the phone book? Because of the need for trust and security, there is one industry that has been missing from the list—financial services. Now the Bitcoin protocol can disrupt the trusted third party of financial services, allowing peer-to-peer lending, banking, and transacting to flourish.

What's at Stake?

The Bitcoin threat is a complete disruption of the status quo. In its purest form, both central banks and commercial banks are no longer needed. Moreover, service providers like Visa, MasterCard, and American Express have their entire franchise at stake. If the Industrial Revolution was the catalyst for modern economies to move from an agrarian to a manufacturing society, then the Bitcoin is the vehicle that will transport the financial system from centralized to decentralized.

Prior to the Industrial Revolution, one third of Americans worked in agriculture; today, that number has plunged to only 1.1 percent. However, technological advances have allowed agricultural workers to be vastly more productive and grow more food. The agricultural industry is an excellent example of how technology can change the dynamics within the industry without reducing output. Unfortunately, during the transition, many workers are displaced. As the financial system moves toward decentralization, it is likely that the ranks of those employed in this industry will shrink. At the same time, those who embrace decentralization will flourish.

In 1919, Frank Little and Alva Kinney pieced together four grain mills to form a company called Nebraska Consolidated Mills. This company embraced the technology of the Industrial Revolution and used it to expand a flour-milling business into one of the largest food processors in the world. In 1971, Nebraska Consolidated Mills changed its name to ConAgra and is the proud owner of such brands as Reddi-Wip, Slim Jim, Chef Boyardee, PAM, and Orville Redenbacher, to name just a few. It stands to reason that somewhere there is another Frank Little and

Alva Kinney rolling up four financial service companies and preparing to build a decentralized behemoth.

According to the U.S. Department of Commerce, in 2012, 5.87 million people worked in the financial services industry, which represented about 6 percent of the labor force. These 5.87 million people produced $1.24 trillion of services or 7.9 percent of U.S. gross domestic product (not including real estate). Bitcoin provides the tool to shrink the amount of the labor force working in financial services, while at the same time maintaining or even increasing the output. This is a multidecade process, so those in financial services have time to adapt, but make no mistake—change is coming.

For centuries, transportation involved what appeared to be an efficient use of horses and carriages. Coachmen would use a buggy whip to spur the horses into a faster pace, and then along came the steel horse (railroads) and the horseless carriage (automobiles). These disruptive technologies not only made the horse and carriage quaint; it made the buggy whip obsolete. Today's buggy whips are credit cards.

Credit card companies' raison d'etre is/was to easily transfer value from one party to another. Credit cards not only offered convenience but also security. Cash is a bearer instrument that means whoever holds it owns it. Credits cards require signatures and second forms of identification; this is known in the alternative currency world as dual encryption. For this service, MasterCard, Visa, and American Express not only charge their customers for the privilege of using the card, they also charge the merchant 2 to 3 percent for privilege of accepting the card.

Figure 5.4 is from CoinDesk's State of Bitcoin Q1 2014 report. They have identified the most likely companies to be disrupted by Bitcoin.

What's striking about this analysis is not just the size of the industry about to be disrupted, but that this analysis does not include the banks. Recently, I needed to transfer money to a business partner in Europe. The cost to complete this transaction at Bank of America was over $50 and would take two business days, not including my time to drive to the bank and fill out paperwork. I chose instead to send bitcoins—with the click of a mouse the payment was sent instantly, without any paperwork and for free. The disruption is not a futuristic thought experiment; it has already begun.

Market Caps (millions) as of 8 April 2014

Processors	Market Cap
Visa Inc	$104,744
American Express Co	$94,486
MasterCard Inc	$82,378
Capital One Financial Corp	$43,930
DISCOVER FINANCIAL SERVICES	$27,418
Alliance Data Systems Corp	$13,968
Total System Services Inc	$5,619
Global Payments Inc	$4,904
Euronet Worldwide Inc	$2,100
Heartland Payment Systems Inc	$1,440
Green Dot Corp	$732
Total	**$381,720**

Payment Hardware	Market Cap
NCR Corp	$5,921
MICROS Systems Inc	$3,892
VeriFone Systems Inc	$3,680
INGENICO	$4,807
Diebold Inc	$2,530
Outerwall Inc	$1,822
Wincor Nixdorf AG	$2,300
Agilysys Inc	$284
ON TRACK INNOVATIONS LTD	$74
Total	**$25,310**

Money Transfer/ATM Outsourcing	Market Cap
Western Union Co	$8,826
Euronet Worldwide Inc	$2,100
Cardtronics Inc	$1,670
MoneyGram International Inc	$1,195
Xoom Corp	$685
Total	**$14,476**

Bank Software	Market Cap
Fidelity National Information Services Inc	$15,455
Fiserv Inc	$14,582
Jack Henry & Associates Inc	$4,743
ACI Worldwide Inc	$2,251
Total	**$37,032**

Figure 5.4 Bitcoin Aims to Disrupt a $459bn+ Industry
SOURCE: CoinDesk, Wedbush Securities.

When Western Union supplanted the Pony Express, it was because they provided a superior product in the form of a faster way to transport information. Likewise, the steel horse and horseless carriage increased the speed of human transportation. The increased ease and speed of transferring value using Bitcoin has the potential to increase the speed of value transportation, aka the global economy.

When the stock market crashed in 1929, news first spread via the Western Union ticker, then the telegraph, and finally the next day in the newspaper. We all watched the horrors of 9/11 on our television screens and immediately flooded the cellular phone networks with calls. When Captain Sullenberger courageously guided his ailing plane into the Hudson River, Twitter was there to capture the miracle.

In business school, the first thing a young capitalist is taught is that there are three ways to gain market share: (1) make a superior product, (2) sell an existing product for cheaper, or (3) do both. The recent breach of the Target card network highlights why a distributed network like bitcoin is superior. All the credit data Target collects is stored in one

database. Thieves only needed to hack into a single point to access the information—a single point of failure. The bitcoin network is decentralized, meaning the information is not stored in a single database. Each transaction must be verified by multiple members of the network and your personal information is never needed. Bitcoin not only offers a superior product; it is also cheaper. In fact, it is free.

As the speed and ease of information transfer increased, so, too, did the information technology business. Telegraphs led to radios, which morphed into televisions, which became connected to the Internet and gave us companies like Netflix. A decade ago, few could have predicting that binge-watching TV on demand would be a multibillion-dollar industry. Likewise, as the ease and speed of value transfer increases, new industries and companies will be born.

Central Banks

The bitcoin transaction I completed with a business partner in Europe is uncharted territory for global central banks. When looked at from a money supply perspective, this transaction reduced the money supply in the United States and increased the money supply in Europe. This occurred without the use of the Federal Reserve, the European Central Bank, or intermediary commercial banks. The only record of this transaction is in the blockchain, but the blockchain does not identify whether the transaction crossed national borders. Therefore, the only record that money flowed out of the United States and into Europe are the words I have written.

While my single transaction is unlikely to have deleterious impact on global monetary policy, as more transactions take place with bitcoins, money supply statistics may become inaccurate. Central bankers who develop elaborate econometric models to guide policy could be missing a major chunk of international transactions. The implication of the missing data is that monetary policy could be based on bad data and could result in bad policy. This scenario may frighten some and delight others. Austrian School purists may rejoice in the free flow of capital, while others may clamor for accountability.

This change need not be frightening, but it does need to be recognized by central bankers. The Bitcoin economy and ecosystem is sufficiently small enough to not have a major impact on money supply. Central bankers have time to incorporate alternative currency transactions into policy decisions and econometric models. The first attempts may simply be guesses, but that should not deter future inclusion. As the financial system moves toward decentralization, the role of central bankers may change dramatically. We already know that transactions are changing global money flows. Central bankers must begin to embrace and understand these flows.

Bitcoin Is the Catalyst

We will never know if Satoshi Nakamoto thought of the implications of his invention. After all, the first computer scientists to use phone lines to send data files were simply trying to make their life easier; they did not realize they were inventing the Internet. While it took time for the Internet to develop into its present form, the revolution was that the Internet decentralized information. Decentralized information was the spark that lit the furnace for organizations like Google and Wikipedia. These organizations disrupted media, publishing, advertising, and even your local library. However, decentralized information also had a problem; namely, anyone could post invalid information. This problem meant that one type of information (financial transactions) could not be decentralized, until Bitcoin.

Bitcoin solved the problem of sending financial information over the Internet without a middleman, and it could serve as the catalyst that decentralizes financial services. A decade from now the financial services industry may employ a fraction of its current labor force, but it will also be much more efficient. This is a change that parallels the move from an agrarian to an industrial economy. The catalyst for this change is Bitcoin and the solution it provides. Through automation the global economy boomed during the Industrial Revolution. In a similar way, Bitcoin, the blockchain technology, and the miners automate many of the functions of our current financial intermediaries. Moreover, the automation

is distributed to anyone who has an Internet connection. Transferring the role of the trusted third party from the financial intermediaries to individuals will not happen without tremendous angst and reluctance.

Those who embrace the change may be rewarded like the early industrialists. Henry Ford and Andrew Carnegie recognized a change and clinched a place in the business hall of fame. Perhaps a spot in the hall of fame will open up for those who take advantage of the Bitcoin Big Bang, or perhaps the financial intermediaries will adapt. What is clear is that over the next decade, creative destruction will be the mantra within financial services, and it will all be due to an anonymous genius who gave his/her/their invention away for free.

Chapter 6

What Do You Call a Bitcoin Miner? A Banker

> [Virtual Currencies] may hold long-term promise, particularly if the innovations promote a faster, more secure and efficient payment system.
>
> —Ben Bernanke

The sun is peeking over the horizon and the fog is lifting off the bay. Your hot cup of coffee steams up the windshield as your car struggles to start. It is cold, it is dark, and it is 11 A.M. Welcome to the bitcoin mines of Reykjanesbaer, Iceland. After checking in with a guard protected by bulletproof glass, you enter the man trap—a chamber that is typically found at a penitentiary. The door slams shut and you think to yourself, "We're not in Kansas anymore" … or maybe you are. Emmanuel Abiodun has a similar setup in Kansas City. Mr. Abiodun is the 30-something CEO and founder of CloudHashing, a global bitcoin mining company.

Emmanuel Abiodun was working at HSBC in London when he heard about a "scam" that was called bitcoin mining. That's right, the founder of one of the largest bitcoin mining operations in the world thought it was a scam when he first heard about Bitcoin. Who could blame him? An anonymous computer programmer wrote 31,000 lines of code so that every 10 minutes any computer connected to the network could hazard a guess at a complex mathematical equation. If the computer guessed correctly, 50 bitcoins were sent to the wallet residing on the hard drive. If it took more than 10 minutes to guess the answer, the software code adjusted the equation so that it was easier to solve.

Between January and March 2013, the price of a single bitcoin began to climb from $15 to $45, and this caught Mr. Abiodun's attention, as it had mine. He set up a computer in the guest room of his suburban London home, downloaded the Bitcoin-QT, and became a bitcoin miner. As the price ascended through $100 on its way to $260 by April 2013, Emmanuel Abiodun's enthusiasm for the project soared. Unfortunately, so did his electric bill.

The further he progressed into bitcoin mining, the more he realized that making real money would require a faster computer running the mining software constantly. Mr. Abiodun continued to work his day job, while his nights were spent adding graphics cards to his mining "rig" and repairing the overheated fan. The operation became so complex and generated so much heat that his in-laws would no longer visit. Not being able to have her parents visit was the last straw for Mrs. Abiodun. She gave an ultimatum—either the computers went or she did.

Emmanuel Abiodun is not the only bitcoin miner to have a problem with heat and a high electric bill. A chemistry professor in Minnesota has set up his mining rig in the basement next to the chimney to help vent some of the heat. A young man in Las Vegas had to buy a second air conditioner just to keep his apartment livable. When his monthly electric bill went from $250 to $700, his wife voiced her skepticism.

But why do these miners even exist? Surely they must have some function to be so handsomely rewarded for upsetting their wives. In order to explain the function of the miners, it's best to look at the guts of a Bitcoin transaction. Fair warning to the reader: We are going to use terms like *nonces, cryptographic hashes,* and *blocks*. Don't worry, we will

make it as painless as possible, but it is a necessary evil to continue our journey.

How Does a Bitcoin Transaction Work?

We will begin with the simple transaction between Keith and Alan. These two young men would like to conduct a Bitcoin transaction—in fact, Keith would like to send Alan one bitcoin as payment for landscaping completed by Alan. Both Keith and Alan have Bitcoin wallets on their computer, and it is in these wallets that their addresses are stored. Your wallet is akin to your bank account. It holds both your bitcoin balance and your addresses. A Bitcoin address is no different than a check; it contains your routing number, account number, and a check number. However, Bitcoin users can create as many addresses as they want and can assign any amount of bitcoins to each address. See Table 6.1.

A Bitcoin address is a 27- to 34-character alphanumeric string that begins with a 1 or a 3 and represents a destination on the Bitcoin network. A typical Bitcoin address looks like this: 13uRbMgunUpShBVTewXjtQTBv5MndwfXhb.

When Keith sits down at his computer, he uses the Bitcoin wallet to create a new address that contains one bitcoin. At the same time, Alan creates an address that allows him to receive the payment and he sends this string of numbers to Keith. In layman's terms, Alan's address says, "Yo, send my bitcoin here." Keith hits send, which instructs the Bitcoin software to send one bitcoin from his address to Alan's address.

Inside Keith's wallet the software is creating both a private key and a public key—this is known as a *cryptographic key pair.* The private key is like the key to your car. If you are selling your car, you must transfer that to the buyer. In the Bitcoin world, the private key shows ownership of

Table 6.1 Bitcoin Components and Functions

Bitcoin Component	Function
Wallet	This is your bank account
Address	These are your checks

the bitcoin. The software signs the transaction with Keith's private key (known only to Keith's computer) and then broadcasts the public key to the Bitcoin network. The public key allows anyone listening to the Bitcoin network to verify that the transaction is coming from Keith's wallet. When the public key and private keys match, voila—transaction verified.

Who are these people listening to the network? Yep, you guessed it, miners. Without the miners nothing gets verified. The computers that Emmanuel Abiodun runs in Iceland bundle all the transactions from the last 10 minutes into a file called a block. The miners' job is similar to a banker's. They transfer ownership from one customer to another and verify that both customers are entitled to transact.

Continuing with the Keith and Alan transaction, if this payment were made with a traditional bank, the banker would verify that Keith has enough funds to be transferred and then facilitate the transfer. Using the centralized Federal Reserve System, the banker would debit one account and credit the other, of course taking a fee for his troubles. With Bitcoin the transaction is free or nearly free. The miners are paid with new coins minted by the Bitcoin software. Functionally, there is no difference between a bitcoin transaction and a payment made with a check. In both cases, money is transferred from one party to the other. The revolutionary difference is that Bitcoin enables the same function without the cost of a middleman.

But wait, aren't the miners the middleman?

This is in fact true; the Bitcoin protocol replaces the banker with the miner and by doing so removes the cost of a middleman. The traditional role of the banker was to be a trusted third party, watching every transaction and verifying validity. Satoshi Nakamoto designed a way for a computer to replace a banker. Bitcoin can accomplish this task securely through the use of cryptography.

What Is Cryptography?

Cryptography is a technique used to enable secure transmission of information. In simple terms, cryptography turns information from a readable state into nonsense and then provides a means to unscramble the

message. This branch of mathematics has been around for centuries and has grown in sophistication as computer scientists have become involved. The predecessors to modern cryptologists were the code breakers employed by armies during times of war. Bitcoin uses cryptography to scramble a financial transaction, transmit it over the Internet, and then unscramble it when it reaches the recipient's wallet. Bitcoin uses a cryptographic hash function to accomplish this task.

The complexity of the term *cryptographic hash function* is second only to the mathematical equation it describes. A cryptographic hash function is nothing more than a mathematical equation that turns words into numbers. It takes any worded message and turns it into a unique string of numbers—think of it as a meat grinder for messages. The message (meat) goes in, the sausage comes out; but in this case, the butcher can use math to turn the sausage back into meat. What's unique about a hash function is that the message or input can be of any length, but the output is a fixed length. This makes sending the message secure and efficient.

Cryptographic hash functions were not invented with Bitcoin. They have a long history of use in digital signatures and e-commerce. In fact, the Bitcoin software is just a really secure way to digitally sign a check, and, in fact, your digital signature is harder to forge than your regular signature. These digital signatures are so unique that the likelihood of someone having the same digital signature is incredibly small.

A digital signature is a way to electronically sign a message. When you sign something using a digital signature, you generate a signing key that is private and a verification key that is public. Using a hash function, your digital signature and your message are mathematically turned into a sequence of numbers, which is now your digitally signed message. To verify the message the decoder needs the signed message and the verification key. Now the verifier (or miner) works backward using the verification key and the signed message. Using math again, the miner can determine if the signed message could be made by combining your private key and digital signature. Since the signature is part of the message, every single message is unique, and this message is broadcast to the Bitcoin network for verification.

The miners then go and check the blockchain to trace whether this digital signature has been used before and what message was sent with it. If the message is identical to a message recorded in the blockchain,

then the miners know that it has been used before and is counterfeit. If the miners do verify that the message is unique and has never been used before, then they allow the transaction.

How do we know that the miners actually did their job and are not being lazy? High electric bills. To solve the cryptographic hash, mining computers must expend a tremendous amount of computational power, which uses a lot of energy. At each moment in time, the Bitcoin network is recording how much computational power is being used to solve the problem; this is called the amount of hash. Anyone can look at the network and determine that mining computers are consuming a lot of electricity to solve the problem—in Bitcoin and cryptography, this is called proof-of-work.

Proof-of-work shows that someone engaged in computational effort. It's a puzzle that, once solved, proves you did the work. Another potential use for the proof-of-work concept is to deter SPAM. If it takes energy to send and decode a message, then it will cost money to send SPAM. It might cost a fraction of a penny to send an e-mail with proof-of-work, but it could cost a fortune to send millions this way.

The encoded message sent to the Bitcoin network is also known as a challenge. When the mining computer listening for a message hears a challenge, it comes up with a response. This response is essentially a guess at the answer to the mathematical equation. The answer to the equation is so rare that it is has only one proper response. Additionally, that response is so difficult to find that it should take the fastest computer 10 minutes to come up with the correct guess.

The process of mining can be compared to flipping a coin, except that the miners flip a massive number of coins—about a trillion—to determine the correct response string. The correct string is what is called collision resistant, which means the chances of two messages being the same or "colliding" are mathematically very low odds. The hash, or mathematical equation, is then applied to both the message and the response. If the hash function outputs the same result, then the miners have verified the message.

The Bitcoin software uses a cryptographic hash function to turn the block of transactions into fixed-size alphanumeric string called the hash value. Now what's special about a cryptographic hash function is that any change in the input creates a completely different output, also called

Table 6.2 Cryptographic Hash Function SHA-256

Input	Cryptographic Hash Function	Output/Hash Value
Send $10	SHA-256	46ab27f445d603f5c33f2153f1faabdc9064fc72e503ec4ae9234c96eec651a6
Send $20	SHA-256	d84d6c04b78f6f3ba2ab62426dc741e57e917c342461a0e54b2c6046f431796a
Send $300.05	SHA-256	bfa7dfc4590dfd62647fca561103e4fee5631e9d0ff9329ff969e0e2a3146556

the digest. In Table 6.2 we used the Bitcoin cryptographic hash function, known as SHA-256 to translate three slightly different messages.

The first thing to notice about the encrypted messages is that changing the message by one character from "Send $10" to "Send $20" results in a vastly different output. The small change in input resulting in a complete transformation of output is one way Bitcoin transactions are ensured to be unique. The second thing to notice is that even if we change the length of the message from seven characters "Send $10" to eleven characters "Send $300.05," the output is still only 64 characters. In fact, any length message will be converted into 64 characters, which makes sending an encrypted message very efficient. Since the blockchain is storing every message, using a cryptographic hash function to reduce messages to 64 characters helps keep the data stored to a minimum.

Each time the message is put through the meat grinder (or hash function), a different output occurs. However, in order to make every transaction unique, the Bitcoin software adds to every transaction a random number called a *nonce*. This random number creates a uniquely different translation, or hash value, for each transaction.

Furthermore, as an additional level of security, the Bitcoin software requires that the hash value begin with a certain number of zeroes. It is impossible for the miners to predict which nonce will produce the correct number of leading zeroes, so they try them all. In fact, every second, all the mining computers on the Bitcoin network compute 10 quadrillion hash values! By brute computing force the miners eventually find a value that matches the randomly generated hash value of the

transaction. In order for a transaction to be confirmed, six miners must find the exact same value.

As more transactions are added to the chain, each block contains a reference to the previous block. If someone wanted to spend the bitcoin that Keith sent to Alan, they would not only have to perform the laborious task of finding the correct hash value, but they would have to go back and refind every hash value for every single transaction that has ever taken place—a virtually insurmountable task. The larger the blockchain gets, the more secure it becomes.

Still Want to Be a Miner?

Mining bitcoins is not just a way for a secure consensus to be reached; it is also the way bitcoins are minted. The first miner to find the correct hash value is rewarded with a block of coins. The original reward was set by the Bitcoin software to be 50 coins, and this amount is cut in half every 210,000 blocks. The current bounty is 25 bitcoins. In addition to new coins, the miners receive a small transaction fee for their work. At the current rate, the transaction fee is negligible, but as more coins are mined the transaction fee will become a larger part of the miner's revenue stream.

Now you might have a spare computer in your attic and are thinking about joining the digital gold rush. Maybe you have an understanding significant other, or maybe you don't care—I am not here to judge. Unfortunately, the meteoric rise in the price of bitcoins has caused an avalanche of interest. With all the new miners, the difficulty level of the network has outgrown simple mining rigs.

Recall when we were talking about how six miners had to confirm the transaction and the average time was about 10 minutes—well, if six miners do it quicker than 10 minutes, then the Bitcoin software makes the math problem even harder. This is what is known as network difficulty. See Figure 6.1.

The hash rate is the dark gray line and is an estimation of how many equations are being calculated every second. As you can see, the rising price attracted more miners, which increased the number of equations being calculated. Since the game of mining is competitive, more players

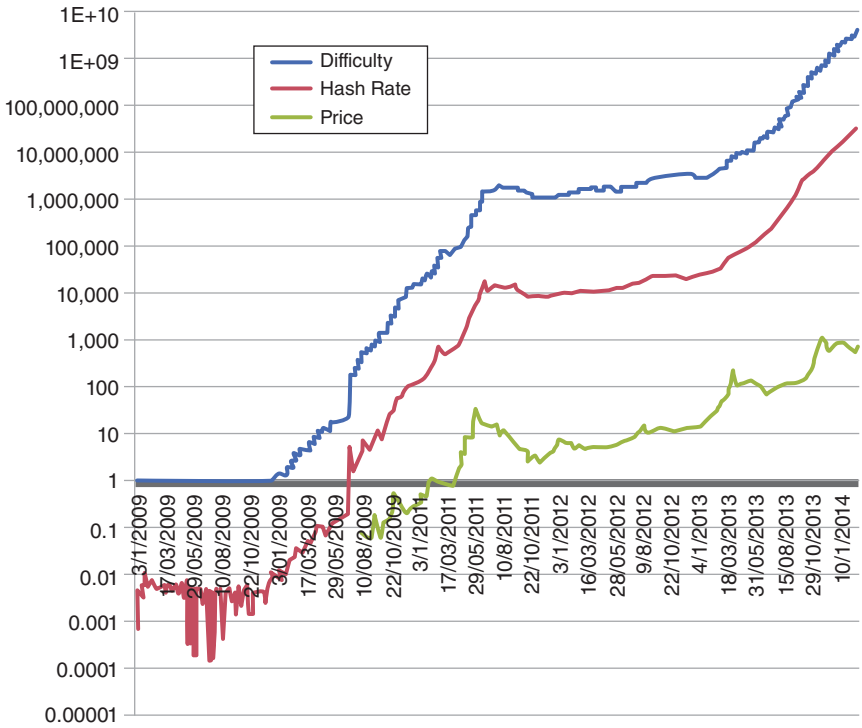

Figure 6.1 Bitcoin Price versus Network Difficulty and Hash Rate
DATA SOURCE: Blockchain.info.

mean faster transaction verifications. The software then adjusts to make the equation more difficult. It was designed this way to keep the creation of the new coins at a constant pace.

With all those calculations you might be thinking that all the coins will be gone by the time you are reading these pages. Think again. The combination of the difficulty adjustment and the block halving rate ensures that the last block of bitcoins will not be mined until 2140. Every 210,000 blocks, the reward gets cut in half. This is known as the block halving rate. But turn that frown upside down; there is still time for you to make your mining fortune. Let's examine what it's going to take.

Since Bitcoin has only been around since 2009, there is a brief history of mining. Consider this your lesson called "A Brief History of Bitcoin Time." A short time ago in a galaxy that resided on the Internet, bitcoins

Figure 6.2 Homemade FPGA Mining Rig

were mined with simple computers; the central processing unit (CPU) was used to solve the math problem. Then a young whippersnapper came along and realized that math problems could be solved faster with a graphics card—yes, while you were enjoying a cold one on the Fourth of July, someone was thinking about how to solve a cryptographic hash faster. Starting to see why they are millionaires?

The next evolution in the mining rig history was FPGAs, or field-programmable gate arrays (Figure 6.2). While this name sounds formidable, what it really meant is that the hardware could be bought in bulk, connected together, and programmed in the field. It might be best to think of this evolution as the MacGyver Age—miners would buy the FPGAs and build a computer that was used only for solving math problems and collected bitcoins.

We are currently in the Gilded Age where Emmanuel Abiodun uses application-specific integrated circuits (ASICs) to crank out cryptographic hash values at mind-numbing speeds. This is how the network is able to complete 10 quadrillion calculations every second. No longer do miners have to jerry-rig computers; the ASICs are factory built to perform. It's not too different than the NASCAR story—moonshiners

Figure 6.3 Dave Carlson in His $8 Million per Month Bitcoin Mine

fixed up old cars to make them run faster. Eventually, they took them to the beach to race. The racecars of today are a far cry from the originals, but the story is the same.

Emmanuel Abiodun is not the only bitcoin miner to build a massive operation. In the state of Washington, Dave Carlson runs one of the largest bitcoin mines in the world (Figure 6.3). Carlson was drawn to Washington because this region has some of the lowest electricity rates, which allows him to generate $8 million a month in bitcoin mining revenue. Yes, $8 million per month! To generate this revenue he uses about 1.4 megawatts of electricity, which is also enough to light up a small town.

Still interested? Let's say you have procured the biggest, baddest rig known to the mining world—maybe you're the person who paid $20,600 for a $1,500 mining rig on eBay. You still may have a tough time making any money. Remember, bitcoin mining is a race. The winner gets the spoils, and winning means having the most computing power. But don't lose faith. There is a way to make some dough—join a club. More specifically, join a mining pool.

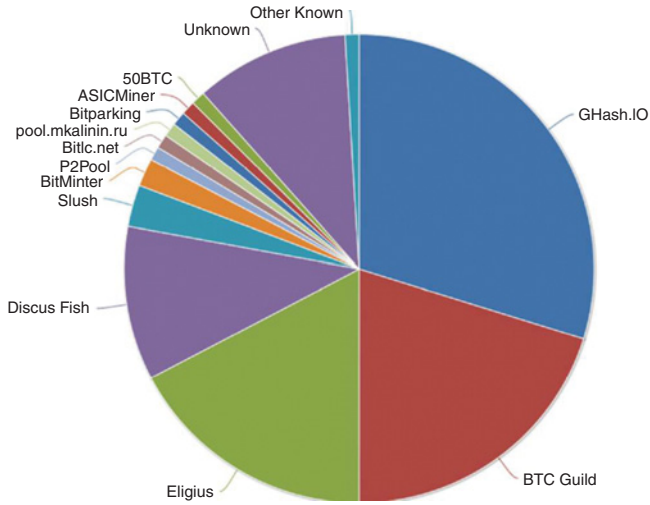

Figure 6.4 Bitcoin Mining Pool Market Share
SOURCE: Blockchain.info, January 10, 2014.

A mining pool is a group of individuals who decide to pool their computing power to mine bitcoins and split the profits. In the Bitcoin world, these go by the clunky moniker *decentralized autonomous organizations*. Don't forget this term—it is key to the future of Bitcoin. For now, just know that the buddy system works. See Figure 6.4.

And just like at the quantum level, the macro (pool) level means the biggest pool with the most power wins. Some of you are intrigued, some of you are about to fall asleep, and yet others see a loophole. First of all, WAKE UP. Okay, now on to the loophole called a 51 percent attack, which we discussed in Chapter 4.

Theoretically, someone or a pool could gather enough computing power to calculate 51 percent of all the equations. If this occurred, then this group would be the only group that could confirm transactions, and they would get all the coins. But even more nefarious, they could confirm transactions twice for the same coin. Not bad, right? Not only do they get all the coins; they get to spend them twice.

Take another look at that pie chart. See the big blue piece of pie? That's a mining pool called Ghash.io. In January 2014 it represented

42 percent of the computing capacity on the network. The Bitcoin community was aflutter. What were they going to do? Was this a nefarious group of bandits or simply like-minded well-meaning miners. The first reaction was a miner's boycott, and true to its self-policing nature, the white-hatted miners began removing their computing power from the pool, thus reducing its influence. Ultimately, Ghosh.io issued a statement that said they had no intention of orchestrating a 51 percent attack and would take measures to avoid such an outcome.

Now with all these pools and supercomputers, you would think miners are making money hand over fist. After all, once the cost of the machine is covered, you should literally be "printing" money. Don't forgot how many who came before you were faced with an ultimatum from their significant other—either the machine goes or they go. That's because the machines are working so hard and use so much energy that they give off a tremendous amount of heat. To keep the operation running, miners use fans and air conditioners, and this is also why Mr. Abiodun moved to Iceland. What does Iceland have in abundance and is essentially free? Cold air. So while the revenue per operation of miners is declining, operations that can use less energy to cool the machines have an advantage.

Let's suppose you don't want to leave your family and they are not particularly keen on moving the Iceland. Is all hope lost? Nope, you can still become a cryptocurrency miner by choosing Litecoin or another digital currency. Wait, what? There is more than one "bitcoin"? Remember when we went deep into the encryption of Bitcoin and we talked cryptographic hashes? Sure you do. Well, a former Google employee named Charles Lee thought that he could improve Bitcoin, and in 2011 he created and released Litecoin.

There are three primary differences between Litecoin and Bitcoin. First, Litecoin blocks are produced every 2.5 minutes as opposed to every 10 minutes with Bitcoin. The advantage to the faster block creation is faster confirmation time and thus less time for a double spending attack. The disadvantage is that all those blocks make a very big chain; thus, the amount of data that must be stored is almost four times that of Bitcoin. Second, Litecoin will eventually issue 84 million coins (recall that Bitcoin will have a maximum of 21 million coins). Third, Litecoin

uses scrypt as an encryption protocol, which makes it easier to mine without a fancy graphics card. The difference between scrypt and SHA-256 used by Bitcoin is how the computer processes the mathematical equation. It is this ease of mining that has led to the explosion of alternative cryptocurrencies, aka alt-coins.

Do We Need Another Bitcoin?

You may be asking yourself why we need another Bitcoin—even more, why would anyone accept an Auroracoin, Dogecoin, or even a BKoin? Professor Robert Shiller has opined that there is a flaw in alternative currencies: none of them solve an economic problem. For long-term success any business must solve a problem. Don't like almonds and coconut? Fine, there is Mounds. Problem solved and empire built. Bitcoin did solve the Byzantine Generals' Problem, and there is unquestionably value in that achievement. However, if miners are to replace the financial service intermediary, then the coins they mine must have an economic purpose.

The other criticism of Bitcoin and alt-coins alike is the lack of stability. On any given day, Bitcoin's price can fluctuate by more than 20 percent. This volatility limits its ability to act as a medium of exchange and a store of value. There are two primary drivers of the volatility: speculators and miners. Since miners need to pay those high electric bills, they are constantly selling and converting digital currencies into fiat. On the other side are speculators who are subject to the whims of human emotion.

There is an old saying about gold: one ounce will always buy you a nice suit of clothes in London. This adage highlights the buying power stability of gold and is one of the primary reasons it has served as a currency over the past 5,000 years. This stability in purchasing power is desired by both the consumer and the merchant. From the perspective of the consumer, stable purchasing power means savings can accrue without the deleterious effects of inflation. A merchant will prefer a stable currency because her profit margin is a direct function of the cost of her supplies. A wildly fluctuating currency means wildly fluctuating cost of goods sold.

The long-run stability of gold is often used to criticize Bitcoin by comparison. Serving as a store of value is one of three essential functions of a currency. If only there were a way to solve this "store-of-value" problem—perhaps if a central bank were involved. The cryptocurrency community will scream blasphemy at the mention of a centralized authority figure. However, if someone could devise a way to stabilize a cryptocurrency using a predetermined algorithm, then problem solved and empire built? Perhaps. In the next chapter, we will follow my creation of the Nautiluscoin, the first coin with its own stability fund.

Chapter 7

Nautiluscoin—0 to $1 Million in 60 Days

All money is a matter of belief.

—Adam Smith

"Freedom is more precious than gold." This was the motto inscribed on the 1776 Georgia pound. When George Washington crossed the Delaware, it was unlikely that he had a pocket full of U.S. dollars. The currency of the land was the Continental currency, or Continentals, issued by the Continental Congress to pay for the Revolutionary War. When the Continental Congress issued this currency, they were not treading on virgin ground. They were, in fact, following a long history of currency issuance that began with the Massachusetts pound in 1690. Codfish bills and Connecticut and Virginia pounds all were in circulation and could be converted into the international currency of the time, which was in 1690 the Spanish milled dollar.

It was not until the National Banking Acts of 1863 and 1864 that the U.S. dollar began to act as the sole currency of the land. The 1863 Act, also known as the National Currency Act, was designed to solve the problem of inflation caused by an abundance of privately issued bank notes. The act taxed the notes issued by state and local banks and effectively made them inferior currency. Taxing private currencies eventually removed them from circulation.

The system of state and privately issued currency worked well until inevitably an economic downturn would make it too tempting to print more notes. The first 150 years of the United States is marked with many episodes of high inflation due to an oversupply of privately issued money. Bitcoin solves the problem of oversupply by mathematically limiting the number of coins that will ever exist. It is this property that makes Bitcoin an ideal subject for private money issuance.

A plethora of doctoral dissertations have advocated for a better system of money, and a few have even argued that the government should not have a monopoly on issuing money. The most well-known advocate of private money was Friedrich Hayek. In his book *The Denationalization of Money* (Institute of Economic Affairs, 1976), Hayek advocated that money should be privately issued and should compete for acceptance. Hayek envisioned a competitive market for private money that converged upon the most stable currencies. He surmised a currency that gained purchasing power would hurt debtors, while a devalued currency hurt creditors. He concluded that the market would choose the currency with the most stable purchasing power.

Not surprisingly, Hayek's suggestion raised a few eyebrows and made him a lightning rod for criticism. The pitfall of economics as a science is that there is rarely a laboratory to test hypothesis. Therefore, economic theory remains just that—theory.

Hayek suggested that a private issuer of money should set a floor on the price of that money to maintain stability. He also suggested that the floor may never be breached as long as speculators believed the central bank was capitalized sufficiently to maintain that floor. This theory has been tested many times with currencies pegged to predetermined levels. The flaw in pegged currencies has always been capitalization of the central bank. Once it becomes evident that the central bank will not be

able to maintain the peg, a speculative attack occurs, forcing the bank to stop buying currency.

One of the more memorable currency peg failures, Black Wednesday, occurred in the United Kingdom in 1992. Currency speculators, including George Soros, had sold short British pound sterling and reaped profits of over $1 billion in a frantic 24-hour period. In anticipation of the Economic and Monetary Union, Europe created the Exchange Rate Mechanism (ERM) to reduce exchange rate variability. The ERM was a semipegged system; that is, currencies were allowed to trade within a predetermined band.

When the ERM was established in 1979, the United Kingdom declined to participate. Since the British pound was free floating, it was subject to the whims of international currency flows. When Nigel Lawson became Chancellor of the Exchequer, he advocated a fixed exchange rate and used West Germany's low inflation record as his reasoning. This admiration and belief in a stable currency resulted in a semiofficial policy of shadowing the West German deutsche mark from 1987 to 1988. However, this policy and the ERM were unpopular with Margaret Thatcher's economic adviser, Alan Walters. When Walters called the ERM "half-baked," Nigel Lawson resigned.

John Major succeeded Lawson as Chancellor of the Exchequer and convinced the British government to enter the ERM in 1990. When the United Kingdom entered the ERM, the deutsche mark was trading at 2.95 to the pound, which meant that the rate could not fluctuate above 3.127 or below 2.773. When currencies are pegged, it means that their economic policies are also twinned. At the time, the United Kingdom was fighting inflation and its economy was on the edge of recession. Germany was also fighting inflation, but its economy was stronger than the United Kingdom's. In order to fight inflation, Germany raised its interest rates to 15 percent, which exacerbated the weakness in the British economy.

As the British economy faltered, the pound sterling began to fall to the lower end of its permitted band. This decline meant the U.K. government had to act or withdraw from the ERM. Acting meant buying British pounds in the open market, and to accomplish this, Britain needed foreign currency reserves. When buying a foreign currency,

one exchanges one currency for another; in this case, the sellers were exchanging the British pound for other currencies like the deutsche mark. In order to facilitate this exchange, the United Kingdom needed a hoard of marks.

However, John Major believed that withdrawal from the ERM and subsequent devaluation of the pound would lead to even higher levels of inflation. Therefore, John Major's initial move was not to withdraw from the ERM or to buy British pounds. He decided to raise interest rates to 10 percent in an attempt to discourage speculators from selling the pound. It did not work.

On September 16, 1992, the United Kingdom announced it would raise interest rates again from 10 percent to 12 percent, but the pound kept falling. Late that same day, the government promised to raise rates to 15 percent, but credibility had been lost. By 7:00 P.M. the United Kingdom announced it would leave the ERM and keep rates at 12 percent.

When the dust settled, it was estimated that the U.K. Treasury had lost over £3 billion trying to defend the currency. The crisis took political and economic tolls, which led many to believe it fueled the recession. With the passage of time, some grew to believe that Black Wednesday was necessary to rebalance the U.K. economy. Regardless of the conclusion, this was a real-life example of what can happen when a central bank loses credibility.

Creating the Coin

When I conceived Nautiluscoin, I was mindful of the pitfalls of a pegged currency, but digital currencies still need a mechanism to reduce volatility. My solution was to create the first digital currency with its own "central bank." The sole purpose of the central bank was to stabilize the currency. I was intrigued and inspired by the possibility to test Friedrich Hayek's theory that consumers and merchants would converge on the most stable currency. The Nautiluscoin Stability Fund is a self-funded "central bank" charged with stabilizing the currency, with the goal of a sound and stable growth pattern, just like a nautilus shell.

What follows is my journal from creation to $1 million in 60 days.

March 6, 2014—Today we had the initial production meeting for the *Fast Money* segment on creating the coin. I sent slides and definitions to the production team yesterday, but they were not as clear as I had thought. Perhaps writing the book and getting into the nitty-gritty of cryptocoins has me a little too close to the project. The goal is to create a 90-second segment that will introduce the world of digital currencies and illustrate how they are created.

The plan is to create the coin using Coingen.io, and then I will premine the coin to create the fund that will act as the central bank. The segment will end with the premine beginning, and then it is up to the power of the central bank to create a liquid and stable market. I have decided to rename the stability fund a "central bank." I think this is the easiest to understand.

Also realized this evening that I either need to pick an official exchange or post an official exchange rate on the website. I think placing a bid in every exchange the coin trades on could become untenable if indeed the coin is successful. For now, I am circling around the idea of an official exchange rate posted on the website.

April 4, 2014—It's been a few weeks but we are getting closer to launching the coin. It is clear to me now that I will need to pick an official exchange for the Nautiluscoin Stability Fund (NSF) to operate. I had an excellent conversation with the founders of Austin Global Exchange. They appear to be exactly the type of entrepreneurial partners that would work well with Nautiluscoin.

Austin Global will be the official exchange upon launch and the NSF will operate on that exchange. The NSF is the name of the central bank I created. After much thought, it seemed incongruous to have a decentralized currency with a "central" bank. The NSF will have the sole purpose of acting as a speed bump when volatility increases.

(*Continued*)

April 12, 2014—We filmed the segment for *Fast Money* this week and are ready to launch the coin. Austin Global Exchange has set up Nautiluscoin so that it can be traded on the day we air the segment. I still believe that creating a liquid and stable market will be the most difficult part of this process. The only reason to buy Nautiluscoin is speculation that it will be accepted by merchants. If the NSF can create a market, then merchants will be more likely to accept.

April 13, 2014—Nautiluscoin just had a heart attack! The team at Austin Global Exchange has found a major flaw in the code that will allow miners to hoard all the coins within the first two weeks and then control the blockchain. I am not sure I really understand what they have found, but I better learn fast!

Update: I have just learned a huge lesson about "Bitcoin Time"—that is how fast things move in this business. When I originally created the coin with Coingen, the software simply cloned Bitcoin (or in Nautiluscoin's case, it cloned Litecoin). The problem is that the original Litecoin code did not account for application-specific integrated circuit (ASIC) miners. The original code adjusts the mathematical problem every two weeks to make sure the problem is being solved within the one-minute time frame I specified. However, the new ASIC miners can mine so fast that before the problem is adjusted they will be able to mine all the coins. They will be able to mine the blocks in mere seconds, not the one minute I originally wanted.

The fix for this is something called Kimoto Gravity Well (KGW)—this is the first time in my life I have heard these words, and I am clearly over my head. After some quick research, I have learned that KGW changes how hard the math problem is after every block instead of every two weeks. In order for Nautiluscoin to become more than an experiment, I will need to install KGW.

April 14, 2014—After speaking with a few digital currency developers, I have determined that KGW will not be able to be

implemented before the launch. I will have to launch the coin with the flaw and take my chances with the miners. At least I will be able to test the efficacy of the NSF; if I can create a liquid and stable market with a huge flaw in the code, then when it is fixed the coin will be even stronger.

April 18, 2014—The coin has launched, and surprisingly it has not been destroyed by miners yet. While I was able to get a lot of attention from the *Fast Money* segment, I don't think the mining community is aware of Nautiluscoin. Also, the price may not be high enough to attract large miners, which may give me time to fix the problem.

To that end, the founders of Austin Global Exchange have put me in touch with the coin developers of a coin called DigiByte. Apparently, they have a better solution than Kimoto Gravity Well—it is called DigiShield and has been implemented in Dogecoin.

April 23, 2014—I have spent the last few days speaking with Jared Tate of DigiByte and I am quite impressed with him. The DigiByte team is going to implement DigiShield into Nautiluscoin, but it is going to take a lot more work than I originally thought. The old code that I received from Coingen will not work if I want to have a robust coin that will be accepted globally—the DigiByte team has to completely recode the coin, and we will have to relaunch the coin. I have to say, the team at DigiByte are very professional and knowledgeable. I think I will buy some DigiByte, as they are the real deal.

Now I am even happier that few people know about Nautiluscoin, as a relaunch means the original coins will be worthless. If a lot of large miners held the coins, they would have wasted energy on mining without getting any return. I hold most of the coins since I am the only miner on the network, and thus a relaunch will not bother me.

(*Continued*)

April 26, 2014—Now that I have a development team working on the code, I can focus on the marketing. When I originally launched the coin, the only place I announced it was on CNBC, but the digital currency community was still unaware. The place to announce a coin launch is the Bitcointalk forum. I have never used this and suspect I will face another steep learning curve.

May 1, 2014—It's relaunch day! We are starting at $0 again, but the code is solid and this will be the first coin to launch with DigiShield. Jared Tate of DigiShield has contacted a few mining pools to be on board for the launch—without these mining pools transactions will not be verified and the whole network will come to a halt. I have learned that a fair launch is very important when establishing the value of a coin. The alternative currency world is filled with pump-and-dump schemes; therefore, new coins are viewed with skepticism. Also, premined coins are looked upon badly, as most people think the developer of the coin is simply going to dump the coins on the market to make a quick profit.

I have announced the launch on Bitcoin talk, and I hope I have explained the NSF well enough that people will understand it is a not-for-profit concept.

1 P.M.—The coin is launched! I just bought the first coins at 0.00400 BTC, which gives it an initial valuation of about $0.18. This is much higher than I expected, but now I need other speculators who wish to purchase from the NSF so that I can use the bitcoins to support the price.

May 2, 2014—The price has plummeted overnight from $0.18 to about $0.9. I just learned a very valuable lesson and discovered a flaw in my stabilization plan. The concept of the NSF is based on the flawed assumption that all holders of Nautiluscoin hold it for the same reason—speculation that merchants will accept it in the future. However, this is not the motivation of the miners—their motivation is to make a profit and pay

their electric bills. Miners couldn't care less about stability, and as soon as they mine the coin, they sell it. I did not anticipate the influence of the miners' selling on the price of the coin.

May 10, 2014—The price of the coin has stabilized, albeit at a very low price. Operating the NSF has become more a job than I anticipated—these markets are open 24 hours a day 7 days a week. It is Saturday night at 11 P.M., and I have just received word that the Austin Global Exchange has been hacked and the holdings of the NSF are in jeopardy. The team at AGX has taken the site down to prevent further security issues—at this point I have no idea if the NSF coins have been stolen.

Update: **12 midnight**—Austin Global Exchange has told me that the holdings of the NSF are secure, but I may have had some bitcoins stolen. I did not have much value in bitcoins at the exchange, so I am relieved that they were the only coins stolen. The exchange is going to stay closed until they figure out the security breach and how to fix it.

May 12, 2014—Austin Global Exchange is back up and running, and the NSF coins that were deposited at the exchange are all accounted for. I have been very impressed with the response from Austin Global—they handled this breach as true professionals. However, I have learned yet another valuable lesson—no matter how secure exchanges appear to be, they are the weak link in the digital currency world. This is an issue that must be remedied if digital currencies are going to become a new asset class.

As luck would have it, Nautiluscoin has been added to another exchange, Poloniex. I had never heard of this exchange, but the addition is welcome, as it is clear that using one exchange for the NSF operation is not secure.

May 16, 2014—The price of Nautiluscoin has more than doubled in the past 24 hours, and the reason is that another exchange has decided to list Nautilus. Mintpal exchange is one

(*Continued*)

of the largest digital currency exchanges, and listing here has caused the price to jump from $0.12 to above $0.25. I still find it curious that simply being added to an exchange adds intrinsic value, but to the extent that a more liquid market adds to the network effect, I suppose there is an argument to be made for the increased valuation.

May 20, 2014—I guess all good things come to an end, even in digital currencies—the price of Nautiluscoin has dropped again by more than 50 percent. As more miners joined the network, more coins were minted. In order to pay electric bills, miners automatically sell the newly minted coins and turn them into fiat currencies. I did not anticipate the influence of miner selling on the price of Nautiluscoin.

The NSF cannot keep up with the selling, and a major flaw in my logic has been discovered. I made the assumption that all holders of Nautiluscoin were holding the coin for the same reason, that is, capital appreciation. Based on this assumption, I thought that controlling the volatility would be much easier than it has turned out. My mistake was to not include the miners' selling in my logic—they don't care about capital appreciation; all they care about is making a short-term profit.

Despite all my marketing efforts to explain the NSF, the miners continue to sell automatically. It is likely that the miners have no idea about the NSF; they are simply looking at a profitability equation. I am sure I will look back at this as a glaring newbie mistake—live and learn!

In retrospect, I should have changed the way the coin is mined from a proof-of-work to a proof-of-stake. The proof-of-stake method removes the miners from the process and allows anyone who holds the coins to mine new coins simply buy holding them in their wallet.

June 12, 2014—The price of Nautiluscoin has slowly dropped lower, and the NSF is not able to soften the blow.

We have been hit by a confluence of events—first, miners continue to mint new coins and dump them on the market; second, the price of bitcoin has dropped 12 percent in just a few days. This has forced the miners to sell even more Nautiluscoin. Since Nautiluscoin cannot be directly converted into fiat currency yet, miners must first sell Nautiluscoin and receive bitcoins. Once they receive the bitcoins, they sell them for U.S. dollars, euros, pounds, etc. As the price of bitcoin drops, the miners need to sell more to pay bills and profit. This negative feedback loop is impacting the price of Nautiluscoin as miners sell more to get more bitcoin.

Unless I find another "natural" buyer of Nautiluscoin, it will slowly grind lower. I need to find a reason for people to buy Nautiluscoin besides speculation that someday a merchant may accept it as payment.

June 17, 2014—The Goddess of Fortune has smiled on Nautiluscoin once again—last evening I was contacted via Twitter by professional mixed martial arts star Jon Fitch. He has just recently become involved in digital currencies and is looking for a sponsor for his next fight. The next fight will air on July 4th weekend on NBC and has the potential to reach millions of households. When Dogecoin sponsored a NASCAR race car, the price of the coin doubled.

June 18, 2014—Jon and I have worked out the details of the sponsorship—the size of the logo is directly proportional to the amount of money paid. I want the community to be a part of this promotion; this will allow anyone with Nautiluscoin to help sponsor the first professional athlete to be paid in digital currencies.

I will start the fundraising by sending 20,000 NAUT to Jon, and then I will announce to the community that we have struck this deal and that anyone can participate. If we can get to

(*Continued*)

$10,000 in U.S. dollar equivalent, then Nautiluscoin will have prime placement on the shorts, shirts, and banners for the fight.

Here is the official announcement:

> We are excited to announce that Nautiluscoin will be sponsoring Jon Fitch, the No. 2 Mixed Martial Arts (MMA) World Ranked Welterweight, in his upcoming fight on July 5th on NBC. Like many of us, Jon has recently caught the digital currency bug, and with this sponsorship he will become the first professional athlete to be paid in a digital currency.
>
> With this sponsorship Nautiluscoin begins its journey toward acceptance as a medium of exchange. In the next few months retailers will be able to accept Nautiluscoin for both online and offline transactions. As well, several new ventures will be launched that will use Nautiluscoin exclusively. This is an exciting time for digital currencies, and Nautiluscoin is fortunate to have such a supportive community.

June 22, 2014—The Jon Fitch promotion has gone very well. Not only have we raised almost $5,000 worth of Nautiluscoin, but the price of Nautilus coin has almost doubled since the announcement. We have taken the total market value of Nautiluscoin from $0 on May 1, 2014, to $500,000 on June 22, 2014.

While all things appear to be going in the right direction externally, internally the coin is having problems. The DigiShield code we used to protect against miners sabotaging the coin is being gamed by those very same miners. The miners are waiting for the mathematical equation to become very easy, and then they throw all their computing power at the coin in an attempt to mine more coins. When the miners turn the computing power toward Nautiluscoin, DigiShield begins to make the equation more difficult and the miners retreat. The problem occurs when the miners retreat. The mathematical equation stays difficult for too long a period, and without the extra

mining power, transactions are not processed. Instead of taking one minute to process the transactions, it is taking hours.

There are two solutions to the problem. The first is for me to become a miner and maintain the network. The biggest hurdle here is that I have do not have the high-powered mining computers, and if I did, I am not sure I would know how to operate them! The other solution is to switch from proof-of-work to proof-of-stake. In proof-of-stake the miners are replaced by the holders of the coin, as long as they can prove they have held the coin, then their computer is used to process transactions. I am inclined to move toward proof-of-stake, as it allows Nautiluscoin to pay a "dividend."

Since my goal is to make Nautiluscoin the investment of choice for professional investors entering the digital currency space, I think proof-of-stake and the "dividend" will be easy to understand. As well, it means the coin is not at the mercy of the miners.

July 5, 2014—It is the day of the big fight, and even though we did not raise the full $10,000 equivalent, Jon Fitch has decided to cover the other half and make Nautiluscoin his primary sponsor for this fight. I had hoped to have the new proof-of-stake code implemented by now, but it is taking longer than expected. Nonetheless, the price of the coin has soared, and in 60 days we have reached a market cap of $1 million, and Nautiluscoin is the 35th most valuable digital currency in the world out of over 300 currencies.

This seems like an appropriate place to end this journal. It has been a successful launch, and I could not be happier with the support Nautiluscoin has received. The community built around the coin is tremendous, and I have learned that building a strong community is essential to coin success.

While we have been successful in getting Nautiluscoin recognized, there is still a lot of work to be done. The next step

(*Continued*)

> is to build the Nautiluscoin ecosystem—this will take the entire community to achieve. There are currently two projects that I know of that are being built around Nautiluscoin as the exclusive means of payment.
>
> The challenge for me now is to build an economy essentially from scratch. This task is both exhilarating and daunting. …

Did It Work?

The creation of Nautiluscoin began with my desire to test the economic hypothesis of Friedrich Hayek. Digital currencies are the perfect laboratory to test his assertion that consumers and merchants will gravitate toward the most stable currency. In the case of Nautiluscoin, there were both some successes and failures. Nautiluscoin successfully grew from tens of thousands of lines of code to one of the most valuable digital currencies in existence. Starting on May 1, 2014, Nautiluscoin had a market cap of $0, and only one exchange was listing the currency. The digital currency speculative community embraced the idea of a stable currency and pushed Nautiluscoin to $1 million in market cap by July 2014. Within 60 days eight different exchanges traded Nautiluscoin, and several other currencies were developed to trade exclusively as a pair with Nautiluscoin. In my view, this is nothing short of remarkable and illustrates that there is some merit to Hayek's assertion.

However, I failed to recognize the impact of miners selling Nautiluscoin to make a quick profit. I incorrectly assumed that all holders of the currency had the same time horizon and reason for holding. This false assumption made Nautiluscoin far more volatile than I anticipated. However, my error in logic does not render the entire experiment a failure; it simply means that going forward the stability fund must factor in all the stakeholders in Nautiluscoin. On several occasions the stability fund was able to halt a precipitous drop in price. The simple act of placing a large buy order on the exchanges made the sellers adjust their behavior.

As I build the Nautiluscoin economy, the stability fund will be modified by the lessons learned in this initial phase. Most notably, the role of the miners can be eliminated by changing the code to what is known as proof-of-stake. In a proof-of-stake system, the holders of the coin do the mining. In fact, one must hold coins in their wallet to prove they have a stake in Nautiluscoin, and only then are they allowed to verify and process transactions. A proof-of-stake system rewards the coin holders for processing transactions and eliminates the miners. Another feature of the proof-of-stake system is that a "dividend" can be paid. That is to say that if an individual holds the coin for a predetermined amount of time and participates in processing transactions, then he or she is paid in newly minted coins, also known as a "dividend."

The Nautiluscoin economy will be built around a stable currency. The initial phase has morphed into something much more than an experiment. There is enough evidence to suggest that Hayek's assertion did indeed change human behavior. Now the task is to build an economy around this finding and further explore the real-world function of this theory.

Chapter 8

Building the Nautiluscoin Economy

The truth is no online database will replace your daily newspaper.
—Clifford Stoll, *Newsweek,* 1995

Currencies have evolved over the past five millennia from commodity backed to government backed. Seashells, animal skins, and shiny rocks have all served as currency and the de facto trusted third party. As governments gained wealth and power, they replaced commodities as the middleman. However, the temptation to devalue fiat currencies has proved to be the Achilles' heel of all government-backed mediums of exchange. This threat of devaluation makes fiat currency an inferior store of value. Since the financial crisis of 2008, many investors have reverted to the protection of gold as a store of value.

While gold has a long history of acceptance as a medium of exchange, its value is based completely on the belief that it can be converted into fiat and accepted for goods and services. There may be a scarcity value of gold, but as the demise of wampum illustrates, scarcity is not the primary driver of a commodity-based currency. When global traders needed to transact outside of North America, they quickly abandoned wampum in favor a currency that was widely accepted. Interestingly, despite the belief in gold as a currency, it is not widely accepted by merchants. In fact, digital currencies are accepted more broadly than gold and are easily transported.

The attributes of global merchant acceptance and easy transport make digital currencies an ideal substitute not only for gold but also for fiat currencies. To be clear, digital currencies do not need to replace gold or fiat to be successful, they simply need to compete with and complement existing mediums of exchange. If digital currencies can take only a fraction of the market share currently held by gold and fiat, then they will be a resounding success.

Nautiluscoin was created to solve a problem and to test a hypothesis. The problem it was designed to solve was my lack of knowledge about the inner workings of digital currencies. Prior to creating Nautiluscoin, I had very little knowledge of hash functions and secure cryptographic algorithms. I needed to get my hands dirty and learn the trade. What I did not anticipate is how much I would absorb. As part of creating Nautiluscoin, I decided to test Friedrich Hayek's hypothesis about private currencies. In particular, I wanted to test his assertion that the most stable currency would be the most attractive currency. During the initial phase of the experiment, I found that Hayek was indeed onto something as investors embraced the idea of a stable currency.

Now that I have established a liquid and relatively stable market, the next task is to develop an economy around this currency. This is backward from how traditional economies and medium of exchanges have developed. Typically, an economy develops around the barter system, then slowly progresses toward a currency-based economy. In this case, I have a currency in search of an economy. I suppose I could take out a personal ad for Nautiluscoin that would read something like this:

NEW KID ON THE BLOCK, SEARCHING FOR THE RIGHT ECOSYSTEM

I have a relatively stable personality and enjoy long runs to increase my purchasing power. I am secure enough to use for serious transactions and I am looking for a professional relationship.

—*GetNauti*

Using the personal ad method, Nautiluscoin may find an economic match or it could just go on endless unproductive dates. The alternative is to go organic and allow the right ecosystem to develop around this stable personality. Creating a fertile environment for an economy to develop requires the continuous pursuit of stability.

The pursuit of stability is not just about reducing daily price fluctuations. For Nautiluscoin to be truly successful it must preserve and increase purchasing power. Daily price stability is important for consumers and merchants to transact, but the long-run success of any currency is a function of purchasing power. If users of a currency believe that their ability to purchase goods and services in the future will be diminished, then they are less likely to hold and use the currency. There are countless examples of sovereign currencies that have gone the way of the dodo bird because of a weak currency policy. Therefore, the most important goal for Nautiluscoin will be to maintain a strong currency with a stable and growing purchasing power.

In order to accomplish our strong currency goal, Nautiluscoin will compete with economics. Traditionally, central banks with a strong currency policy are charged with providing an anchor for the economy through the use of money supply targets, interest rate targets, and/or exchange rate targets. Economic history has shown that these targets require the central bank to have significant resources in order to credibly accomplish the targets. Most successful targeting policies rely on an unlimited resource, which is classically the ability to print or borrow money. In the case of Nautiluscoin, the money supply is fixed by the software code and there are not public debt markets to use as interest rate targets. However, this does not mean it lacks arrows in the quiver.

Because the money supply is fixed and released over time, we have the ability to set the growth rate of the money supply. In addition, the Nautiluscoin network will be secured through the proof-of-stake

method, which allows us to pay interest to those who desire to hold Nautiluscoins. Finally, the mining process allows us to support the exchange rate by using mining profits to purchase Nautiluscoin. Using these three arrows, Nautiluscoin will compete with sound economics and become the "blue-chip" digital currency.

Dynamic Proof-of-Stake

Currently, Nautiluscoin uses a proof-of-work (PoW) method to verify and transmit transactions that is similar to Bitcoin. The PoW methods requires miners solve a very difficult math equation in order to process transactions; for their effort they are rewarded with freshly minted Nautiluscoins. In a proof-of-stake (PoS) system, the holders of the coins perform the role of the banker/miner, and it is these holders who are rewarded with freshly minted coins.

For example, let's suppose a merchant holds 10,000 Nautiluscoins that she received from selling a product. In a PoS system, she is rewarded for holding those coins and broadcasting her ownership to the network. The ownership broadcast is stored in the blockchain and used to verify a valid transaction when she chooses to spend the Nautiluscoins. In practice, the merchant may hold the coins in her wallet for seven days; this information is recorded so that everyone knows these coins belong to the merchant. The information about her stake in the coins is valuable to the network, and this value is rewarded with more coins. In this case, after seven days, the merchant may receive 1,000 more Nautiluscoins, which would make her net holdings 11,000 Nautiluscoins. In this way, the merchant has received an interest payment of 10 percent in seven days—not too bad. At the same time, the "central bank," which is the computer code, has increased the money supply by 1,000 Nautiluscoins.

Continuing with this example, it follows that if the purchasing power of Nautiluscoin has remained stable or increased, then the merchant has received an economic benefit by helping to verify and process transactions. If the purchasing power increases and the merchant received an interest payment, then she may be encouraged to spend the additional income. It is this incentive and feedback loop that will be used to target a rate of growth for the Nautiluscoin economy.

Nautiluscoin Gross Domestic Product Target

The goal of all central banks is to promote economic growth. Typically, central bankers choose a goal of full employment and price-level stability in order to target an economic growth rate. In simple terms, the chain of causality for monetary policy looks like the chart shown in Figure 8.1.

The simple assumption in this basic model of central banking is that money supply growth has a direct linear impact on economic growth. Real-world experience refutes this assumption and suggests that the relationship is dynamic. Moreover, the goal of increasing the money supply may be better defined as increasing purchasing power. For example, if a pack of gum costs $1 today and the U.S. Federal Reserve doubles the money supply overnight, the pack of gum may cost $2 tomorrow. At the same time, however, consumers have twice the amount of money, which means that the $2 pack of gum costs the same as the $1 pack of gum. If a consumer has only $1 today and is given another $1 overnight, and the price of gum increases to $2, the consumer has the exact same purchasing power as he did the day before.

The nonlinear dynamic relationship between money supply and economic growth is why the Nautiluscoin money supply will dynamically adjust to the growth of the economy. A unique feature of digital currencies is that every time a block of transactions is processed, the software records the number of transactions that have occurred. Nautiluscoin processes a block of transactions every minute, which means that every 60 seconds we will be able to tell if the economy is growing or slowing. The rich set of data is massive advantage over fiat currencies and allows for a predetermined set of rules to control the money supply.

Functionally adjusting the money supply every minute is not practical or desirable as the volatility in the amount of transaction would create too much noise to make an informed decision. In the case of

Figure 8.1 Chain of Causality for Monetary Policy

Nautiluscoin, once a month the transaction volume will be analyzed to determine if the economy is growing or shrinking. If the economy is growing at or near the target rate, then the money supply will remain unchanged. However, if the economy is slowing, the money supply will be adjusted to increase purchasing power.

This type of algorithmic approach to monetary policy has been rarely tested in the real world and lives mostly in economic textbooks. Once again, digital currencies are leading the way as the perfect laboratory to experiment with algorithmic monetary policy.

Algorithmic Monetary Policy

In the case of the Nautiluscoin economy, the goal of the monetary policy will be to increase or decrease purchasing power in response to the relative strength or weakness in the economy. To that end, the initial target for Nautiluscoin economic growth will be set at 5 percent a year. If economic growth is falling short of this goal, then the interest rate and money supply will be adjusted to increase purchasing power.

Functionally, how this will work may appear to be counterintuitive, as increasing purchasing power means raising interest rates. Recall that the interest payment is made to those who own and hold Nautiluscoin; therefore, raising the interest rate will encourage more users to buy and hold Nautiluscoin. The new buyers attracted by the increased interest rate must also hold their coins for a predetermined amount of time. This holding period will remove supply from the exchange rate markets and, coupled with new interest rate–sensitive buyers, should increase the price of Nautiluscoin. In this way, raising interest rates not only increases the money supply but also increases the exchange rate, which together will result in a rise in purchasing power.

If the economy is growing faster than the targeted rate, then interest rates will be decreased. Decreasing the interest rate reduces the growth of the money supply and may encourage some holders to sell their coins. As interest rate–sensitive holders reduce exposure the exchange rate should fall resulting in a decrease purchasing power. The goal of the dynamic algorithmic monetary policy is to create a smooth economic growth pattern over the long run, as shown in Figure 8.2.

This dynamic PoS system is possible only because the digital currency software is constantly recording the transaction taking place in the

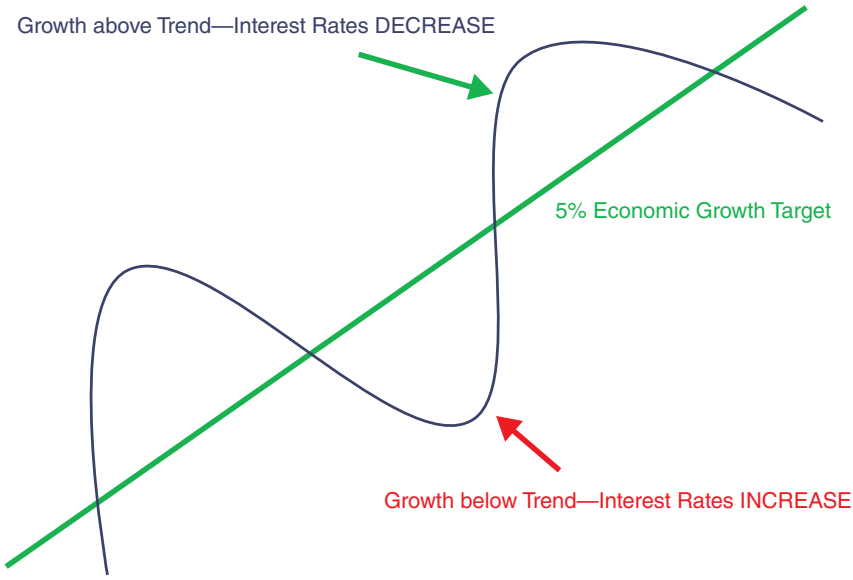

Figure 8.2 Dynamic Algorithmic Monetary Policy Creates Smooth Economic Growth Pattern over the Long Run

Nautiluscoin economy. Currently, central banks rely on government agencies to collect and estimate economic data. Typically, this process is characterized by frequent adjustments of the data by a single point of failure. If the U.S. Department of Labor miscalculates the unemployment rate, monetary policy could be rendered useless. With digital currencies, data about the economy are continuous and secure. That is not to say that digital currencies can improve on monetary policy, just that the data set is more accurate.

Other Policy Tools

In addition to the dynamic PoS system that will be implemented into Nautiluscoin, there are two other tools that can be used to promote economic and purchasing power growth. The first of these tools already exists in the form of the Nautiluscoin Stability Fund (NSF), while the second tool, a PoS multipool, will be implemented with the switch to the dynamic PoS system.

The NSF was conceived to stabilize the price of Nautiluscoin and ultimately increase the purchasing power of the users and holders of the currency. However, I discovered a flaw in my logic when miners began to indiscriminately sell their holdings of Nautiluscoin. I incorrectly assumed that all holders of the coin had the same motivation, that is, holding the coin in order to achieve a return on investment. I did not account for the fact that the miners' motivation is to convert the digital currency to fiat as quickly as possible in order to fund the mining operation.

The switch to a PoS system will eliminate the miners and allow the NSF to fulfill its function of a speed bump for excessive volatility. The NSF will function similar to the way a market maker does in the financial markets. The fund will provide liquidity when it is needed, with the goal of continuously supporting purchasing power. The operation of the NSF in the exchange rate markets does not eliminate the potential for panic or euphoria—those are uniquely human qualities. However, the NSF can provide an unbiased level head during times of extreme human behavior.

The second tool that will be used is a PoS multipool. Even though the PoS method eliminates mining, it does do not preclude us from mining other digital currencies. Recall that a mining pool is a group of miners that combine computing resources. The combination is more powerful than individual miners and thus increases the chances of being the first to solve the math problem and receive the reward.

Originally, mining pools focused on one coin, and thus profits were a function of the fluctuation in the price of the coin. Eventually, miners developed multicoin pools as a way to increase profitability and reduce exposure to currency rate fluctuations. A multicoin pool uses an algorithm to mine the most profitable coins. The algorithm calculates the odds of success in solving the math problem and the price at which the rewards coins can be sold. These multicoin pools are constantly switching mining operations among the most profitable coins.

In a typical multicoin pool, the coin profits are immediately converted into either bitcoins or fiat currency so that the mining operation can stay funded. A PoS multipool does not convert the coin profits into fiat currency; instead, it uses the profits to buy the PoS coin. In the case of Nautiluscoin, a multipool will mine other coins and the profits will

be used to buy Nautiluscoin. In this way, there will be a continuous flow of buying into the exchange rate market. This continuous flow of buying combined with the NSF operation should provide a powerful tool to increase purchasing power.

Alternative to Gold

As the monetary policy tools are deployed, Nautiluscoin should garner attraction from both merchants and consumers. Wide acceptance of Nautiluscoin for goods and services will give it a distinct advantage over gold. Moreover, the three-arrow approach to algorithmic monetary policy could provide Nautiluscoin with more stability than gold. To that end, as the markets develop, the NSF will be used to keep the volatility of Nautiluscoin below the volatility of gold. Low volatility, increasing purchasing power and merchant acceptance, will allow Nautiluscoin to compete against gold as an alternative currency.

The ability of Nautiluscoin to take market share from gold will have a dramatic impact on the price of the coin and by extension its purchasing power. As of 2013, it is estimated that there have been 171,000 tonnes of gold mined in the history of the world. Since gold does not deteriorate, all of this gold still exists. In one tonne of gold, there are 35,274 ounces, which means at $1,300 per ounce the total value of all the gold in the world is $7.8 trillion dollars.

Nautiluscoin's value proposition is that it does not deteriorate, it has a monetary policy that enhances its function as a store of value, and it can be used as a medium of exchange. Gold does not have a supportive monetary policy; in fact, gold's value is a function of perception. Moreover, as a medium of exchange gold falls short since very few merchants accept gold directly. The value proposition will allow Nautiluscoin to compete for market share with gold.

Table 8.1 illustrates the implied value of Nautiluscoin at different levels of gold market share.

If Nautiluscoin attracts just 1.0 percent of the value of gold, then the implied price of Nautiluscoin is $15,682. This is to say if 1 percent of the holders of gold decide that Nautiluscoin is a better store of value and choose to convert their gold into Nautiluscoin, then the

Table 8.1 Nautiluscoin Implied Value

Percentage Market Share	U.S. Dollar Value of Market Share	Implied Value of Nautiluscoin
0.10%	$7.8 billion	$1,568.20
0.50%	$39.2 billion	$7,841.00
1.00%	$78.4 billion	$15,682.00

implied valuation would be above $15,000 (assuming a total of 5 million coins).

Could this increase in market value occur? If Hayek's hypothesis is correct and the algorithmic monetary policy is effective then attracting a portion of the investment dollars from gold is achievable. Since all currencies are a matter of belief, it may take some effort to move those investment dollars. However, as the markets develop and regulation attracts institutional investors the likelihood of success should increase.

Money, Made Better

Ultimately, the impact of all these monetary policy tools will be to provide the fertile ground for an economy to be built around a currency that is economically sound with a transparent policy. To be sure, economics is about more than algorithmic monetary policy and increasing purchasing power. At its core, economics is a social science that seeks to influence human behavior. As a 20-year participant in the financial markets, I am skeptical that human behavior can be controlled. However, much like the butterfly that flaps its wings and causes a hurricane, small changes in monetary policy can have a short-term impact on human behavior.

The Nautiluscoin strong currency policy will be supported by three tools for monetary policy: dynamic proof-of-stake, a stability fund, and a multicoin mining pool, as shown in Figure 8.3.

These policy tools have two channels by which they can influence purchasing power; they can operate through the exchange rate channel

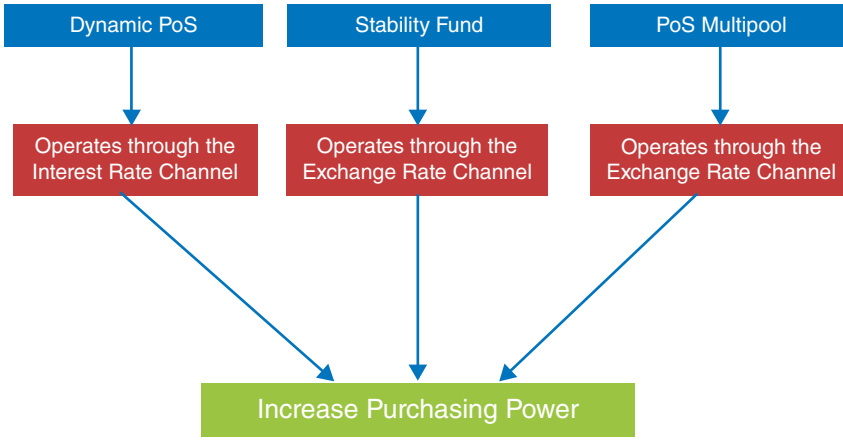

Figure 8.3 Nautiluscoin Policy Tools

or the interest rate channel. Because Nautiluscoin is not a reserve currency, the ultimate determinant of purchasing power will be the exchange rate with fiat currencies and bitcoin.

As the policy is fine-tuned, Hayek's economic hypothesis suggests that consumer and merchant acceptance should grow. As acceptance grows, the ecosystem should follow and Nautiluscoin-specific business can be formed around this stable and sound money. If successful, Nautiluscoin will not only have a robust economy with steady growth, but it will also be a unique time in economic history that a theory of private currency has been implemented.

Financial Market Integration

As Nautiluscoin develops its reputation as the private currency that is an alternative to gold, it should also gain attention from both merchants and consumers. Both user groups should gravitate toward Nautiluscoin as a stable currency with increasing purchasing power that is beneficial to both. However, Bitcoin has a significant lead on all the competition for traditional retail transactions. While Nautiluscoin can compete

technologically, the Bitcoin network effect is a formidable barrier to entry. Therefore, Nautiluscoin will need to find a niche to compete.

The status of the U.S. dollar as a global reserve currency has made it the go-to currency in which to price international commodities and financial markets. However, the current centralized nature of the U.S. dollar network is characterized by middlemen, bank fees, and exchange rate risk. Each of these points of friction represents a reason why the U.S. dollar is not the most appropriate currency for international financial markets. Additionally, each of the friction points represents an opportunity for Nautiluscoin.

To understand how this may work, let's use the example of an oil producer in Canada who wants to sell its oil to a buyer in China. Under the current system, the global price of oil is quoted in U.S. dollars. The Chinese buyer must convert renminbi into U.S. dollars to buy the Canadian oil. Additionally, the Canadian oil producers must convert those U.S. dollars into Canadian dollars in order to pay its employees. Of course, each time a currency conversion is made, an international foreign exchange bank stands in the middle and collects a fee. Moreover, the buyer and seller are losing money on the bid/ask spread in the fiat foreign currency markets.

If the global price of oil were denominated in Nautiluscoin, then the buyer and seller of the oil could bypass many of the middlemen in the international financial markets. To be sure, there would still be an exchange rate risk when converting back into local currency, but the three stability mechanisms for Nautiluscoin should reduce that risk. In addition, a smart contract could be attached to each transaction that specified when and where the value is transferred. When the oil tanker arrives in the Chinese port, the smart contract would trigger payment. This would eliminate the risk of the Chinese buyer paying for oil that never arrives.

In order to facilitate the integration of Nautiluscoin into the financial markets, we will need to establish indexes to be used a reference. The function of these indexes will be to standardize the prices of global commodities and financial markets from U.S. dollars into Nautiluscoin. In this way, we can establish a benchmark for financial markets price in digital currency and remove some the friction from the system.

Special Drawing Rights

The concept of a global reserve currency has been attempted before, specifically with the creation of the International Monetary Fund's (IMF's) Special Drawing Rights (SDRs). Created in 1969 to help support the Bretton Woods Agreement of fixed exchange rates, SDRs allow member countries to freely exchange SDR holdings for useable fiat currencies. SDRs were designed to help countries with strong finances help countries with weak finances and facilitate the flow of currency among IMF members. This could be done voluntarily, or the IMF could instruct its members to buy SDRs from countries that need foreign currency.

Digital currencies and SDRs share common characteristics, notably that they both rely on a network of users willing to accept the currency in exchange for a good or service. However, SDRs are limited by a lack of liquidity and requirement to be a part of the IMF. Moreover, the centralization of the currency within the IMF structure does not make it ideal for international transactions. Finally, the intended purpose of SDRs was to facilitate lending among IMF members, which is a completely different function than a global reserve currency.

Digital currencies, specifically Nautiluscoin, are uniquely positioned to solve the problem of friction within the international financial markets.

Why NAUT?

The early stage of the digital currency ecosystem has been characterized by new coins boasting technological improvements. While this technological evolution is necessary, the competition in this niche is fierce. Fortunately, due to the open-source nature of digital currencies, Nautiluscoin can adapt the most promising technology. The large and diverse community supporting Bitcoin makes it difficult for this original digital currency to be flexible and adapt new technologies. Flexibility is an advantage for Nautiluscoin.

Additionally, the tradition of anonymity in digital currencies may have been useful during development, but the professional investment stage will require transparency. Given the high-profile creation of

Nautiluscoin, it enjoys a level of transparency that is unprecedented in digital currencies.

Finally, the Nautiluscoin economy will be built around the sound economic principles of a stable currency and increasing purchasing power. The unique algorithmic monetary policy will give Nautiluscoin an economic advantage over other digital currencies.

While Nautiluscoin may have been created as an experiment, it has taken on a life of its own. Nautiluscoin has been fortunate to have a strong and active community of digital currency investors who have helped build the early ecosystem. As the steward of this ecosystem, my job is to position Nautiluscoin as the premiere investment in the digital currency asset class. The business plan for Nautiluscoin rests on the three pillars of continuous improvement, transparency, and sound economics.

Chapter 9

Investing and Trading in Alternative Currencies

> With e-currency based on cryptographic proof, without the need to trust a third-party middleman, money can be secure and transactions effortless.
>
> —Satoshi Nakamoto

In the summer of 1944, as war continued to devastate Europe, 730 delegates from the 44 allied nations gathered in the serene White Mountains of New Hampshire. The Bretton Woods Conference, so named because it was held at the Mount Washington Hotel in Bretton Woods, New Hampshire, was convened to design the global system of money after the end of World War II. This conference not only established the World Bank and the International Monetary Fund, it also created a global system of fixed foreign exchange rates. The U.S. dollar was deemed to be the global reserve currency, as it could be converted

directly into gold. All other currencies were pegged to the U.S. dollar in order to give them stability.

In the relative calm of the postwar era, the Bretton Woods System was successful in maintaining global currency stability. The Marshall Plan allowed both Germany and Japan to rebuild and created tremendous demand for U.S. products and by extension the U.S. dollar. However, the success of the Bretton Woods System would be its downfall. As a result of U.S. dollar demand, the currency became overvalued and the United States became less competitive. In the spring of 1971, West Germany was the first country to leave the fixed exchange rate system and the value of the U.S. dollar dropped 7.5 percent from May to July 1971. The drop in the value of the dollar prompted countries with large dollar holdings to convert to gold. When Switzerland and France redeemed a large amount of U.S. dollars for gold the pressure intensified to devalue the U.S. dollar. In fact, the U.S. Congress released a report recommending just this action.

During a frantic secret meeting at Camp David, President Richard Nixon gathered his advisers, and they concluded that the United States should unilaterally suspend the U.S. dollar convertibility into gold. On Sunday, August 15, 1971, President Nixon took the television airwaves and announced that he had taken the United States off of the gold standard. This executive order effectively terminated the Bretton Woods Agreement.

Dubbed the Nixon Shock, the collapse of the Bretton Woods Agreement meant currencies that were once pegged to the dollar were now free floating. With free-floating exchange rates came the development of the foreign exchange markets. These markets were unregulated, fragmented, and illiquid by today's standards. Notably, these same characteristics describe the current status of digital currency markets. In the 40 years that followed the Bretton Woods Agreement, the foreign exchange market became the largest market by volume in the entire world. During this time, fortunes have been made and lost—recall George Soros's billion-dollar triumph over the Bank of England.

In its current form, the digital currency market resemble the fiat currency markets during the 1970s—fragmentation, illiquidity, and a lack of regulation were all hallmarks of the fiat markets. Despite its humble beginnings, the foreign currency market developed into the largest

and most powerful financial in the world. In fact, the Bank for International Settlements reported that in 2013 the foreign exchange markets traded $5.2 trillion per day. Today, foreign currencies represent a way for investors to diversify holdings away from traditional financial markets. Digital currencies have a similar potential to become not only major financial market but also a new investment class.

The Bitcoin Big Bang may prove to be another moment in history like the Nixon Shock. As the economies of the digital currencies evolve it will open up new investment opportunities. Digital currencies are really no different than their fiat cousins—they support the transfer of value in an economy by providing a medium of exchange, a unit of account, and a store of value. Moreover, as the data for these digital economies becomes more accessible, these digital currencies can be analyzed in the same manner as fiat currencies. It would not be surprising to see digital currencies become an integral part investment planning.

A New Investment Class

In 1952, Harry Markowitz introduced Portfolio Theory (now known as Modern Portfolio Theory), which suggested that investors need to take into consideration how each of their investments fluctuated with each other. Markowitz proved that investors who allocated investment funds based on the relative price movement of one asset class with another would outperform those investors who simply focused on individual security selection. Modern Portfolio Theory is the foundation for almost every asset allocation model in use today. At its core the principle suggests that the volatility of an investment portfolio can be reduced by mixing different asset classes together. Moreover, investors should not only look at absolute return but also at how much risk was assumed to generate the investment return.

The simplest asset allocation model is the 60/40 portfolio, which places 60 percent of the assets in stocks and 40 percent of the assets in bonds. Using this formula for asset allocation, an investor would have realized 10 percent a year return from 1990 to 2011 with a portfolio fluctuation of 10 percent per year. That is to say, the portfolio could increase or decrease in value by an average of 10 percent at any

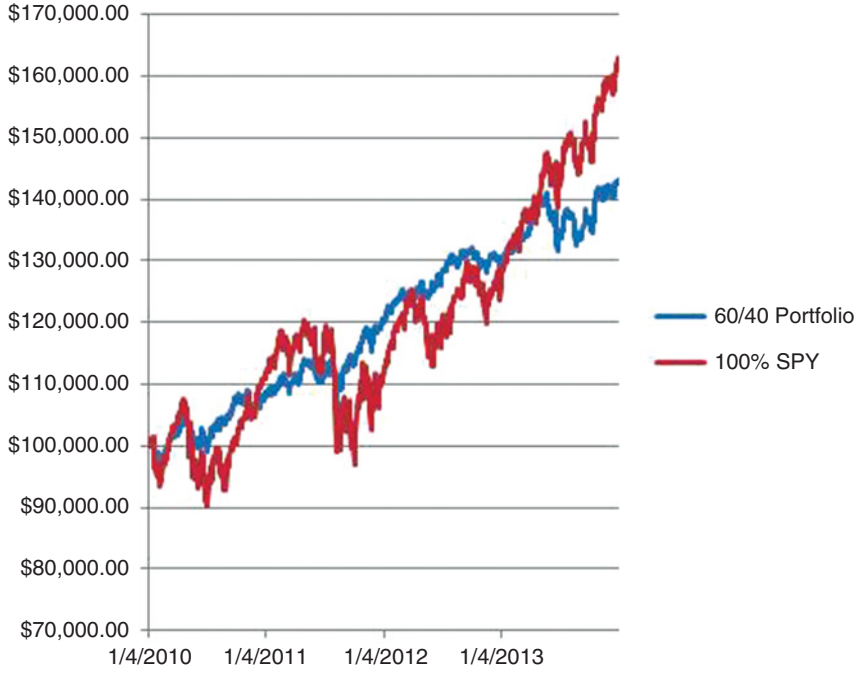

Figure 9.1 A $100,000 Portfolio That Is Invested $60,000 in SPY and $40,000 in TLT

given time in the year. In comparison, the S&P 500 typically fluctuates 19 percent per year. The key to reducing volatility is creating a portfolio of uncorrelated assets. For example, using the SPDR S&P 500 exchange-traded fund (ETF; SPY) and the iShares 20+ US Treasury Bond ETF (TLT) as proxies for stocks and bonds, respectively, we can create a $100,000 portfolio that is invested $60,000 in SPY and $40,000 in TLT. See Figure 9.1.

Since 2010, the 60/40 portfolio returned an average of 9.39 percent while the stocks only portfolio returned an average 13.69 percent. See Table 9.1.

However, the stocks only portfolio was seven times more volatile than the portfolio that allocated to the bond market. As Markowitz suggested, this is because stocks and bonds are uncorrelated assets, when stocks rise, bonds tend to fall and vice versa. Unfortunately, there is a

Table 9.1 Return of 60/40 Strategy and Stocks Only

Year	60/40	SPY
2010	8.50%	11.79%
2011	11.02%	−0.20%
2012	7.41%	13.47%
2013	10.65%	29.69%
Average Return	9.39%	13.69%
Return Volatility	1.73%	12.28%

flaw in Modern Portfolio Theory that has come to light since the Great Recession. Since the Federal Reserve has embarked on quantitative easing, both stocks and bonds have risen together. In practice, this means that these two asset classes are no longer uncorrelated and the diversification benefits have been diminished.

The *Wall Street Journal*, CNBC, and Burton Malkiel, the father of the Random Walk, have raised concerns about the changing correlation. In an interview with CNBC, Malkiel declared the 60/40 portfolio downright dangerous in this environment. As the chart in Figure 9.2 shows, the three-month correlation between stocks and bonds has become positively correlated, while for ideal diversification a negative correlation is best.

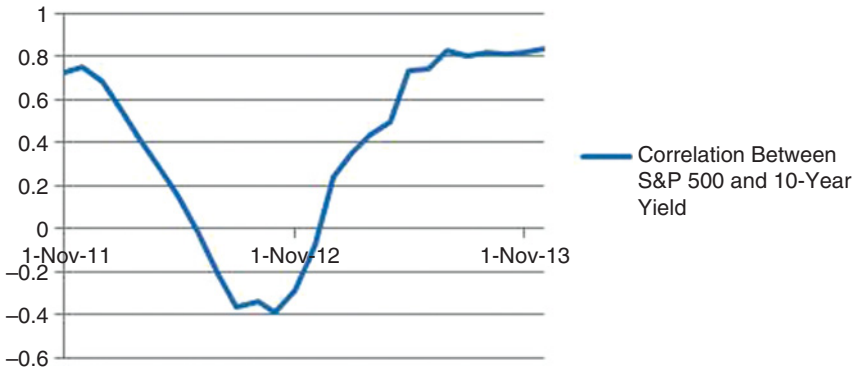

Figure 9.2 Rolling 6-Month Correlation between S&P 500 and 10-Year Yield

Table 9.2 Bitcoin Daily Correlation with Other Assets 2010–2013

S&P 500	Nasdaq Composite	10-Year U.S. Treasury	Gold
0.8030	0.8419	0.3007	−0.6920

In other words, bonds no longer provide the diversification protection that they once did. Bitcoin and digital currencies in general offer a new asset class of potentially uncorrelated returns, which could add to portfolio diversification. See Table 9.2 for Bitcoin's daily correlation with other assets between 2010 and 2013.

Over the past three years, the correlation of bitcoin and the S&P 500 has become highly positive, indicating that bitcoin may not be an aid to diversification. However, from September to November 2012 the S&P 500 dropped almost 7 percent, yet the price of bitcoin increased by 17.3 percent. The divergence in performance resulted in the correlation between the S&P 500 and bitcoin to become negative. The implication is that the current highly positive correlation may simply be coincidence. To be sure, this is anecdotal evidence and the sample size is still too small to make a solid statistical declaration. Nonetheless, the emerging economies of digital currencies have the potential to enhance portfolio diversification.

This new investment class must grow into its promise, as it currently lacks some of the full potential as money. It is generally accepted by economists that "money" has three functions: a medium of exchange, a store of value, and a unit of account. As a medium of exchange, digital currencies meet the requirement for money; currently, over 45,000 businesses accept bitcoin. Startups are popping up each day with the sole purpose of making it easy for consumers and merchants to use digital currencies. Moreover, digital currency acceptance will accelerate with the network effect.

A unit of account means that a certain amount of money can be exchanged for a basket of goods. For example, if your grocery bill is $100 per week, you might say the 100 units of dollar bills accounts for a basket of groceries. The pitfall of all fiat or paper currencies is that inflation erodes purchasing power so that in 10 years your basket of groceries may cost $200. Economists have argued that inflation is

the result of creating more units of account; in other words, printing more money provides a temporary sugar high to a failing economy but eventually leads to inflation. Arguing the cause of inflation is well beyond the scope of this book; however, digital currencies make it impossible to print more units. Recall that the mining slowly releases new units into the ecosystem. It is this steady flow of units that make digital currencies a superior choice as a unit of account.

Some have argued that Bitcoin is not real money because its price fluctuates wildly. Detractors contend that volatility keeps Bitcoin from functioning as a store of value. However, the skeptics miss the point that since we experience inflation with paper money, the stability of a dollar is an illusion. Anyone who used to frequent a penny candy store knows that the U.S. dollar has not maintained a stable value. Because most developed nations experiencing inflation of less than 5 percent per year, the critics have ample ammunition when the price of bitcoin fluctuates 5 to 10 percent per day. However, over time, the U.S. dollar has failed as a stable store of value, and death by a thousand paper cuts has the same outcome as a fatal heart attack.

The volatility of the price of bitcoin will likely drop with acceptance—in fact, increasing usage is already having a dampening effect. As the price stabilizes, there is a strong argument for global commodities to be priced in digital currencies. Because digital currencies do not have a central bank or a government attached, there are no political or monetary obstacles to acceptance. Saudi Arabian oil producers accumulate billions of U.S. dollars, but they have no control over the Federal Reserve or Treasury. At any moment in time the U.S. monetary authorities could decide to devalue the currency. Those holding billions would be disproportionately hurt. The money supply for digital currencies is fixed from the moment the code is written. That is not to say that market forces cannot move the price of the currency up or down due to fluctuations in demand, but monetary authorities cannot change the supply.

The lack of a monetary authority and subsequent inability to pay taxes in digital currencies is another argument against digital currencies as "real" money. The retort to this criticism is that a U.S. citizen cannot pay the IRS with yen or euros, yet they are still currencies. The authority to tax depends on enforcement of property rights, which is typically the

role of a central government. If taxes are unpaid, the government has the right to take your property, whether it is a lien on your house or a garnishment on your wages. If a tradesman does work and is unpaid, she can place a tradesmen's lien, which will be enforced by the courts. These are the rules that we as a community have agreed to live by. Since Bitcoin does not have a central government or an army to enforce the rules, it can never be a currency … or so the argument goes.

What is overlooked is that Bitcoin has its own built-in enforcement mechanism that in some ways may be superior to our current system. Within the Bitcoin protocol is a timestamp—it allows you to program in the time that a payment is made—very similar to scheduling a payment online with your bank account. However, Bitcoin goes a step further and allows you to attach a contract to that payment and both the contract and payment are recorded in the general ledger. Since bitcoin transactions are irreversible once the transaction and contract are digitally signed and recorded, there is no way to default on the agreement.

Agreeing to pay your taxes or an invoice from a plumber is a contract. You may not have signed it, but it is still enforceable by the government. Bitcoin cuts out the middleman (government) and programs the enforcement of the contract (payment) directly into the general ledger. This concept is what is known as a smart contract or smart property. We will learn a whole lot more about smart contracts later, but for now it is important to know that the smart money aspect of Bitcoin is what makes enforcement better than our current system.

To be sure, Bitcoin is a young currency and a new technology, which is both threatening and intriguing. Wall Street has always looked favorably on new technologies in other fields but is slow to adapt to structural changes within its own industry. There was a time that electronic trading was looked upon as unethical—"gentlemen" were supposed to trade over the phone or face-to-face, but now there is an arms race to create the biggest and fastest electronic trading systems.

The current view on Wall Street is that Bitcoin is not a currency but it could be a new asset class, which is Wall Street–speak for "we can charge a fee" for this. If indeed a new asset class is born, then there are new divisions to create, new research reports to issue, and advisory services to be sold. In my view, there will eventually be a digital currency

mutual fund and your financial adviser will have a really nice pie chart that will show you how much you should be investing in alternative currencies as asset class.

Valuation

Whether digital currencies are a new type of asset or a currency, they still need to be valued. Since digital currencies do not have a cash flow associated with them (yet), using a discounted cash flow analysis is not very helpful. It is better to value them as traditional currencies. That is to say, the value should reflect the size and growth of the underlying economy. Given that merchant acceptance is a large driver of value, there is an emerging currency aspect to digital currencies. If we consider an emerging currency a proxy for the underlying good or service provided, then it follows that as the good provided by the emerging economy is more widely accepted the value of the emerging currency increases. For example, look at the country of Chile, the world's largest producer of copper. Overlaying the Chilean peso with the price of copper illustrates that the value of the Chilean peso fluctuates almost directly with the price of copper, as shown in Figure 9.3.

Digital currencies can be thought of in a similar way. As the underlying economy grows—that is, more merchants accept the currency—the value of the currency should grow. In other words, increased merchant acceptance provides natural demand for the currency from new entrants into the market. Figure 9.4 illustrates that the price of bitcoin has risen with the number of merchants accepting bitcoin. The smooth lines are an exponential smoothing mechanism applied to each series. The exponential trend lines indicate which is growing at a faster rate, the price of bitcoin or merchant acceptance.

What's interesting is that the influence of merchant acceptance is diminishing. The rapidly rising dotted line shows that the price is appreciating at a much higher rate than the number of transactions (smooth line). Using this simple indicator, one might conclude that the price of bitcoin is currently driven by speculation. This phenomenon could mean that Bitcoin's success could ultimately be its demise—at least when it comes to the price.

Figure 9.3 HGY00—High-Grade Copper—Daily Line Chart

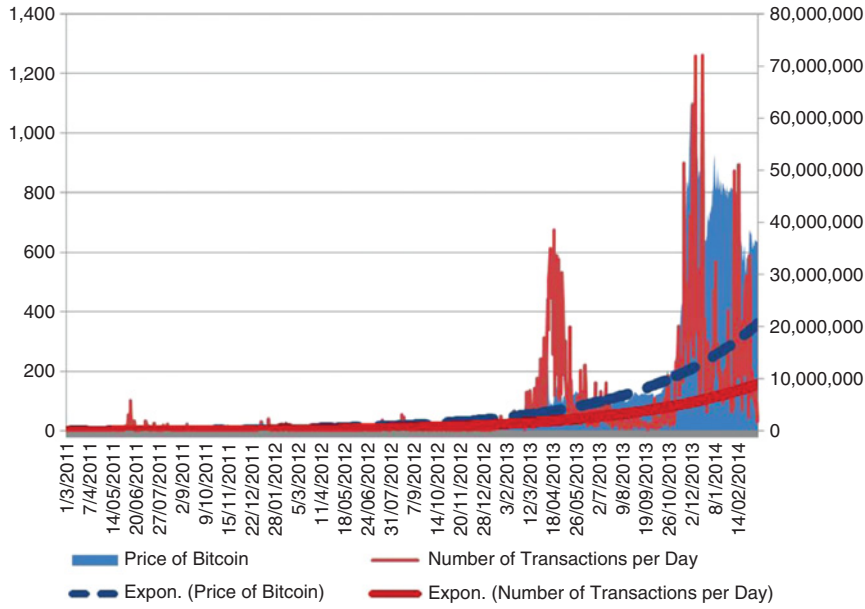

Figure 9.4 Price of Bitcoin Rises

To explore why the success of Bitcoin could be detrimental to the price, let's suppose, in extremis, that every merchant in the world accepts bitcoin and every consumer has exactly the number of bitcoins they desire. Under this scenario the new natural demand evaporates. At the same time, speculation will be quelled by saturated merchant acceptance. Removing the support of both of these natural buyers could have a detrimental effect on the price of bitcoin. Of course, we do not know when or where this will occur—it could happen at $1,000 or $1 million.

This brings up an interesting point about Bitcoin that makes it ripe for a bubble. When transacting, consumers and merchants do not care about the price of bitcoin, what matters is that during the time they are transferring value, the price remains stable. This means that the primary buyers of bitcoin at this point in time (the consumers) are agnostic as to price. Buyers being agnostic to price is a building block of a bubble. Moreover, there is an emerging infrastructure that supports margin trading, which is another essential ingredient for a speculative bubble. The combination of buyers who are price agnostic and the ability of

speculators to use credit to purchase are what all bubbles are built on. It is extremely likely that bitcoin will reach bubble conditions at some point in its lifespan—all markets do—as it is an indisputable fact that humans extrapolate current trends into the future, often with exponential growth. At some point, these expectations become so divorced from economic reality that the bubble pops.

Has the bubble begun? Nope. Merchant acceptance is growing but is not even close to completed; therefore, the price of bitcoin has a long way to run before expectations can be divorced from reality. This also means there is time for investors to add digital currencies to their portfolio, which entails dealing with an exchange or a private investment vehicle. The Bitcoin Investment Trust is one of the private investment vehicles for bitcoin and has published an interesting table on the potential upside to bitcoin valuation, shown in Table 9.3.

This valuation comparison clearly illustrates the incredible upside potential for the price of bitcoin. Using conservative assumptions, the valuation of bitcoin has the potential to increase by 10 to 100 times its current value. This valuation comparison can also be used to evaluate other digital currencies. Bitcoin may have the network effect as a tailwind, but that does not mean another digital currency cannot unseat the reigning king. As a comparison, Google is one of the largest companies

Table 9.3 Potential Upside to Bitcoin Valuation

Bitcoin Upside			
If Bitcoin Equals the Value of . . .	**Basis for Comparison**	**Current Value**	**Implied Price for Bitcoin**
PayPal	Leading online payment network	$30 billion	$3,750
Monetary base of Turkey	Emerging-market currency	$96 billion	$12,015
5% of gold	Primary global store of value	$376 billion	$47,010
Current Bitcoin valuation		$8 billion	~$600

SOURCE: Bitcoin Investment Trust.

in the world and undisputed leader in Internet search. This company, which is ubiquitous in our lives, did not even exist when the Internet became popular in 1994. In fact, in 1999, Google had only eight employees! If we look at Bitcoin as a proof of concept, then it becomes easier to see how a newer digital currency could become the leader.

At this point you may be reaching for your checkbook, ready to invest in the digital currency that may become the next Google. Well, slow down, cowboy. Investing in digital currencies takes a few steps to enter the ecosystem. First, you will need to convert your fiat currency (dollars, euro, yen, etc.) into digital currencies, which can be done at some exchanges and wallet services. Once you have bitcoin, buying and selling other digital currencies is as easy as entering an order to buy the stock of Google.

Exchanges

Digital currency exchanges act as both a broker and an exchange. Additionally, they can be divided into bitcoin-only exchanges and alternative currency exchanges (aka alt-coin exchanges). The bitcoin-only exchanges do exactly what it sounds like—they trade bitcoin only. Well, actually, they usually trade a few of the larger alternative currencies like Litecoin and Ripple. The alternative currency exchanges trade everything else like Nautiluscoin.

In order to purchase bitcoin you will need to use a broker/digital wallet service like Coinbase and deposit fiat currencies. Once your deposit is accepted, then you can purchase bitcoins. As a holder of bitcoins, you are now part of the digital currency ecosystem and can send those bitcoins to any exchange you choose. Once at the exchange, you can purchase a myriad of digital currencies using bitcoins. Most exchanges price digital currencies in either bitcoin or Litecoin, but as the ecosystem has grown, some other currencies are being used to price digital currencies. For example, the AllCrypt exchange prices several digital currencies in terms of Nautiluscoin.

While we are on the subject of exchanges, let's talk about the most infamous: Mt. Gox. At its zenith the Mt. Gox exchange was the largest bitcoin exchange in the world, and its implosion cost people millions

of dollars. Remember when we hinted about hot and cold wallets in a previous chapter? Sure you do. Well, this is where they play a role.

A hot wallet is a digital currency wallet that is connected to the Internet. This allows you to send any digital currency over the Internet in a matter of seconds. The risk is that being connected to the Internet exposes the wallet to hackers. This is why most people keep large sums of digital currencies in what are known as cold wallets. A cold wallet is *not* connected to the Internet—it can be a laptop that is not plugged in or connected to Wi-Fi. Alternatively, a cold wallet can be a server that stands alone with no connection to the outside world. A cold wallet can even be a USB thumb drive that is plugged into a computer only when you want to transfer currency. The key takeaway is that a hot wallet is connected to the Internet and vulnerable, while a cold wallet is not vulnerable to a cyberattack.

How does this relate to Mt. Gox? Glad you asked. Most exchanges hold a majority of the digital currencies deposited in cold wallets. The digital currencies are transferred to a hot wallet only when someone wants to make a trade. Typically, exchanges hold 80 to 90 percent of their deposits in cold wallets, and the rest is used by active traders. In the case of Mt. Gox, they had a large number of bitcoins in their hot wallets, which exposed them to a cyberattack. What's more, Mt. Gox lacked sufficient records and a protocol to determine where all the deposits resided. When word spread that Mt. Gox had been hacked, everyone rushed to pull their coins out of the exchange. However, without sufficient records it was difficult to determine where all the coins were—they had no idea how many coins were in the hot wallet and how many had been stolen.

Investment Vehicles

For some, the idea of a hot or cold wallet and the potential for a cyberattack is more information or risk than they want. The solution is to invest in a regulated vehicle that does all the security and exchanging for you. There are two primary investment vehicles for those who wish to hold bitcoins—one is still waiting approval, and the other is up and running.

Winkelvoss ETF

The Winkelvoss twins—yes, the same ones from the Facebook saga—have applied to create a publicly traded ETF that will hold bitcoins. The approval process for any ETF is long, and an ETF based on bitcoins will likely get extra scrutiny. The advantage of this structure, when it is approved, is that it will provide a liquid trading vehicle for bitcoins. Instead of venturing onto unregulated digital currency exchanges, the Bitcoin ETF will allow anyone with a U.S. brokerage account to buy, sell, and trade bitcoins. Of course, just like the gold ETF, this product is not designed to be "cashed in"; this is simply a way to participate in the price fluctuations of bitcoin.

Bitcoin Investment Trust

If you can't wait around for the Securities and Exchange Commission to approve a Bitcoin ETF and you don't want the hassle of buying and safely storing a large sum of bitcoins, then the Bitcoin Investment Trust (BIT) may be for you. The Bitcoin Investment Trust is a product offered through a wholly owned subsidiary of SecondMarket and is directed at high-net-worth individuals looking to gain exposure to Bitcoin. The main benefit of this fund is that buying and storing can be a laborious task, especially for the uninitiated. Downloading a wallet and then linking a bank account to an exchange can be daunting. The BIT offers a simple way to get exposed to bitcoin in U.S. dollars without the need to become a digital currency expert. This is the perfect investment vehicle for those who want to be early adopters without the learning curve of hot and cold wallets, safe storage, and security codes.

There are a few unique features of the BIT that make it ideal for sophisticated investors. Currently, if you want to buy any quantity of bitcoins, you must deal with several unregulated and unregistered businesses. The operators of many digital currency exchanges are not very visible by design, and they often operate from countries with questionable rules of law. To be sure, some of the larger and newer exchanges are beginning to come out of the shadows, but it is still a business of unregulated entities. At the same time, the market for bitcoins and especially alternative currencies is highly fragmented, which makes buying larger

sums of bitcoin difficult. In an effort to circumvent many of these challenges, the operator of BIT procures and stores bitcoins without your having to deal with the aforementioned players.

The BIT is marketed and distributed by SecondMarket Inc., which is a U.S.-based and Financial Industry Regulatory Authority (FINRA)-registered broker-dealer. Moreover, the BIT is structured so that your ownership is in shares of the trust not directly in bitcoins. Similar in structure to the SPDR Gold ETF, the value of BIT shares are derived from the underlying bitcoins the investment vehicle passively holds. The benefit of this structure is that the ownership title is clear and can be used for estate-planning purposes. Additionally, because the shares of the BIT are securities, they can be held in some tax-advantaged retirement accounts as well as brokerage accounts. This makes obtaining bitcoin exposure in your investment portfolio as simple as instructing your retirement account broker to buy shares in the BIT.

The downside to this structure is that it is illiquid. Since these are private securities, there are certain limitations on when and how they can be sold. Eventually, as the shares in the BIT mature, they will be eligible for trading by the general public. SecondMarket has an extensive knowledge of the private securities markets and is best known for handling much of the pre–initial public offering trades in Facebook stock.

Asset Class Growth

Regardless of how you choose to invest, this new asset class is just beginning to grow. When the Nixon Shock freed fiat currencies to float with market forces, the foreign exchange markets were hardly developed. Eventually, as more liquidity entered the foreign exchange markets and more products were developed, the currency market growth exploded. From over-the-phone trading to lightning-fast computers, foreign currency can now been sent around the world quite literally at the speed of light. Moreover, there are dedicated mutual funds, hedge funds, and financial intermediaries that have all developed over the past 40 years.

The lessons learned from the growth of the foreign exchange markets can be applied to digital currencies, and since there is a preexisting template, it is likely that the digital currency markets will develop faster.

When the Bretton Woods System collapsed, futures and options markets did not exist, yet as these words are being written, futures on digital currencies are being developed. Finally, rapid institutional investor acceptance will come only with regulatory clarity. The current uncertainty over the legitimacy of digital currencies is a roadblock to wider acceptance. Pension funds, insurance companies, and other institutional investors have a fiduciary responsibility to invest in asset classes with a clear legal structure. As this legal structure develops for digital currencies, professional investors will be more likely to enter the market.

Chapter 10

Regulation

> Pull the string, and it will follow wherever you wish. Push it, and it will go nowhere at all.
>
> —Dwight D. Eisenhower

The topic of digital currency regulation is not just controversial; it can be downright inflammatory to digital currency purists. Bitcoin was created to remove third parties from the financial system, whether they are government agencies or money center banks. As a proponent of free-market capitalism, I would prefer the market to self-regulate and many digital currency traditionalists view the self-regulating mathematical code at the heart of these currencies as superior to any government regulation. This argument has merit but also has a flaw in its logic. While the mathematical code does an exceptional job of removing financial intermediaries, it does not address the problem of human greed and deceit.

As the creator of a digital currency, I have watched the industry mature from a terrible toddler with a penchant for the illicit to a

rebellious teenager with a bright future. For digital currencies to fulfill the promise of adulthood, they need some rules to live by—a protocol, if you will.

For the first time in human history, digital currencies and the blockchain technology allows individuals to send secure information over an unsecured network without a trusted third party. The most obvious use for this technology is for financial transactions. Conveniently, the centralized financial-services industry is ripe for disintermediation. Since the founding of the Bank of England in 1694, our financial system has consisted of middlemen orbiting the central banks. This web was necessary to ensure the safe transfer of value between two parties who have no way of trusting each other. The trusted third party, or middleman, performed an essential function by verifying the legitimacy of financial transaction and transferring the value.

However, digital currencies and the blockchain are more than just a medium of exchange; they represent a secure database open to anyone who has an Internet connection. The Internet opened an unprecedented amount of information to society, but it lacked a mechanism to verify the information. The blockchain technology is the mechanism by which any piece of information can be traced back to its source by everyone. This technology is too important to lurk in the shadows.

Law enforcement, taxing authorities, and financial market regulatory agencies all have expressed interest in defining the rules for digital currencies. It is still very early in the game, and many of these regulators are just beginning to understand the scope of digital currencies. The good news for digital currency advocates is that any type of regulation will be an implicit nod of legitimacy. With the swipe of a pen these agencies have the ability to declare digital currencies illegal, but a set of rules means the asset class is here to stay.

Regulatory Agencies

Depending on the geographic location, digital currency regulation has ranged from outright bans to laissez-faire approaches. Iceland and Vietnam are the two countries where Bitcoin and digital currencies are banned. These bans are more about the international capital flows than banning the technology. During the financial crisis of 2008, Iceland

suffered from capital fleeing the economy as the banking system imploded. In order to prevent another crisis, Iceland bans transferring digital currency outside of the country. Interestingly, there is a digital currency that is designed to be used within the borders of Iceland; Auroracoin is legal in Iceland because it is specified to be used only in Iceland.

The two most influential countries on digital currency regulation are China and the United States. Much of the extreme move higher in bitcoin during 2013 was a result of Chinese citizens buying Bitcoin in order to move money out of the country. Since China runs a fixed fiat exchange rate system and restricts capital flows, digital currencies offered a way around the authorities. However, the Chinese government was quick to halt the capital flows by warning state-owned banks against working with digital currency exchanges. In December 2013, the People's Bank of China also blocked payment processors from dealing with digital currency exchanges. These moves effectively stopped the massive outflow of money from China and the price of bitcoin dropped by over 50 percent. This was the maelstrom that turned my "can't-lose trade" in the Bitcoin bubble into a long-term investment and was a catalyst for writing this book.

In the United States, several agencies at both the state and national levels have taken a swipe at regulation and law enforcement. In March 2014, the Internal Revenue Service issued guidance on the tax treatment for virtual currencies. In effect, this guidance treated digital currencies as property like a share stock rather than a currency. This ruling is positive for investors for two reasons. First, it gives clarity on the tax implications of investing in digital currencies as an asset class. It should encourage institutions to move into the space and create a new source of demand for bitcoin. Since the total value of bitcoin is small relative to other asset classes, it would not take many institutional-size investors to push the price up substantially. Second, U.S. investors who hold bitcoin for more than a year will be taxed at the capital gains tax rate. If Bitcoin were deemed a "real" currency, investors would be taxed at their ordinary tax rate regardless of holding period. This should encourage long-term holding of digital currencies and has the potential to reduce volatility.

It is interesting to compare the IRS ruling with the regulatory guidance from Denmark. On December 17, 2013, Denmark's Financial Supervisory Authority (FSA) issued a statement that said digital

currencies would not be regulated by the FSA. Additionally, on March 25, 2014, TV2 network in Denmark reported that the tax authorities determined that gains on virtual currencies would not be taxed. The varying tax treatment of an asset that does not have a legal residence highlights one of the challenges in regulating digital assets.

Another challenge to regulation can be found in the saga of SatoshiDice, an online Bitcoin gambling site. In 2012, the founder of SatoshiDice, Erik Voorhees, launched an initial public offering (IPO) to raise money to develop the site. In this case, the capital raised was in bitcoins, not fiat currency. Additionally, the shares issued to SatoshiDice traded on an exchange called MPEx, which is based in Romania and trades only shares of companies that are priced in bitcoin. Since the shares were offered to U.S. investors (among other countries), the U.S. Securities and Exchange Commission (SEC) charged Erik Voorhees with violating the Securities Act of 1913. This act requires registration of IPOs with the SEC. Even though Voorhees only issued digital assets and raised bitcoin, the SEC found that regardless of the currency used, offering an investment to a U.S. citizen requires registration. Voorhees paid a fine of $50,000 and has sold the website to an anonymous buyer for almost $12 million.

FINCEN

The first U.S. regulatory agency to offer guidance and rules on digital currencies was the Financial Crimes Enforcement Division of the U.S. Treasury (FINCEN). The FINCEN guidance was designed to prevent fraud and financial crimes and focused primarily on money service businesses. A money service business is any entity that accepts currency and performs a money transmission service. Essentially, these guidelines are an attempt to curtail the use of digital currencies by those wishing to obfuscate potentially illegal transactions.

FINCEN Guidance to Prevent Fraud and Financial Crimes

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible

virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person. FinCEN's regulations define the term *money transmitter* as a person who provides money transmission services, or any other person engaged in the transfer of funds. The term *money transmission services* means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."

The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA. FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and decentralized convertible virtual currencies.

The unintended consequence of these guidelines is that it shifted some of the regulatory burden onto the state banking agencies. In doing so, the FINCEN guidelines made it a requirement that money service businesses engaged in digital currency transactions would need to register with all 50 state banking agencies. While the FINCEN guidance was welcomed by the venture capital community as it began to crystalize the regulatory picture, it has placed an unnecessary burden on many businesses and has the potential to stifle innovation.

New York Department of Finance

Fostering innovation was specifically mentioned when in July 2014 the New York Department of Finance became the first state regulatory

agency to submit proposed laws on digital currencies with the announcement of a BitLicense. Superintendent Benjamin Lawsky took the lead in regulating digital currency businesses with the goal of protecting consumers while nurturing innovation. The proposed law requires New York–based digital currency businesses obtain a BitLicense. The BitLicense would make firms to not only keep records on customers but also maintain certain capital levels. Once again, the threat of unintended consequences could derail entrepreneurial spirit in digital currencies. In particular, the compliance, capital, and record-keeping requirements have the potential to drive digital currency businesses from the state of New York.

Section 200.7 Compliance

(a) Generally. Each Licensee is required to comply with all applicable federal and state laws, rules, and regulations.

(b) Compliance officer. Each Licensee shall designate a qualified individual or individuals responsible for coordinating and monitoring compliance with this Part and all other applicable federal and state laws, rules, and regulations.

(c) Compliance policy. Each Licensee shall maintain and enforce written compliance policies, including policies with respect to anti-fraud, anti–money laundering, cyber security, privacy and information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body.

Statutory Authority: Financial Services Law, sections 102, 301, and 302

Few would argue that compliance with anti–money laundering rules is a deterrent to innovation, but the requirement to designate a compliance officer and maintain a written compliance policy will make the idea of starting up a business in New York unpalatable. Unless these rules are adopted by all 50 states, entrepreneurs will simply choose to set up shop outside of New York State.

Moreover, the requirement to maintain certain capital levels is too ambiguous and broad to be useful. There is no doubt that any business that is offering to safeguard the general public's assets should be required to maintain levels of solvency. However, even the rules established by over 300 years of central banking did not prevent the financial crisis of 2008 and the commensurate fraud.

Section 200.8 Capital Requirements

(a) Each Licensee shall maintain at all times such capital as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations. In determining the minimum amount of capital that must be maintained by a Licensee, the superintendent will consider a variety of factors, including but not limited to:

(1) the composition of the Licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset;

(2) the composition of the Licensee's total liabilities, including the size and repayment timing of each type of liability;

(3) the actual and expected volume of the Licensee's Virtual Currency Business Activity;

(4) whether the Licensee is already licensed or regulated by the superintendent under the Financial Services Law, Banking Law, or Insurance Law, or otherwise subject to such laws as a provider of a financial product or service, and whether the Licensee is in good standing in such capacity;

(5) the amount of leverage employed by the Licensee;

(6) the liquidity position of the Licensee; and

(7) the financial protection that the Licensee provides for its customers through its trust account or bond.

The New York Department of Finance would be better served by adopting the rules that already govern financial service businesses. This

would allow digital currency businesses to compete on equal footing with the existing banking system.

Finally the requirement to keep records of every transaction is simply a nonstarter for almost any new business.

> **(1) Records of Virtual Currency Transactions**
> Each Licensee shall maintain the following information for all transactions involving the payment, receipt, exchange or conversion, purchase, sale, transfer, or transmission of Virtual Currency: the identity and physical addresses of the parties involved, the amount or value of the transaction, including in what denomination purchased, sold, or transferred, the method of payment, the date(s) on which the transaction was initiated and completed, and a description of the transaction.
>
> **(2) Reports on Transactions**
> When a Licensee is involved in a transaction or series of transactions for the receipt, exchange, conversion, purchase, sale, transfer, or transmission of Virtual Currency, in an aggregate amount exceeding the United States dollar value of $10,000 in one day, by one Person, the Licensee shall notify the Department, in a manner prescribed by the superintendent, within 24 hours.

If every transaction that took place needed to include the physical address of the parties involved then very few digital currency transactions would take place in the state of New York. The entire point of digital currencies is that they are an efficient means of transferring value. If two parties agree to exchange value, there is not a need to exchange physical addresses. If indeed the records requirement makes it into the final law, two outcomes will occur: first, very few businesses will apply for a BitLicense; and, second, the businesses that do apply will incur large legal and record-keeping fees.

Finally, these rules would be better served if they were accompanied by a tax break for those who receive a BitLicense. The state of New York is already offering tax-free zones with up to 10 years of tax-free

operations, combining these zones with BitLicense zones would offset some of the onerous costs.

Challenges to Regulation

The strength of digital currencies is that they exist on millions of computers distributed across local and international borders. This distribution presents a challenge for regulators since enforcement across local and international borders is virtually impossible. Ideally, regulations will be light-handed enough to encourage those in the digital currency space to voluntarily submit to regulation. The BitLicense needs to be a stamp of legitimacy that is sought after by those operators with the most integrity. Moreover, the critics of regulation will surely point toward the potential for increased costs. This criticism is not without merit and is why it is critical for the New York Department of Finance to honor its commitment to not stifle innovation. Light-handed regulation to protect consumers and allow more people to experience the benefits of digital currencies is a welcome addition to the ecosystem.

Regulation of digital currencies may appear to be anathema to those who subscribe to the purest form of Nakamoto's open-source creation. The open-source nature of digital currencies provides a built-in self-regulatory mechanism, but that mechanism does not protect against human greed. For digital currencies to grow up, they need a set of rules that allows for entrepreneurship while encouraging and protecting new users. Regulation done correctly can not only expand the user base but also implicitly give digital currencies legitimacy.

The digital asset industry has formed a group called the Digital Asset Transfer Authority (DATA), which aims to be an industry liaison with global regulators. DATA works with both industry leaders and regulators to facilitate best practices within the digital asset industry. It is entities like DATA that will become the FINRA of digital assets.

Pushing on a String

With all the new investment products that are being developed it is only a matter of time before more regulations are part of the ecosystem.

Cyberattacks on major digital currency exchanges have threatened to derail the growth of the blockchain technology. Moreover, many venture capitalists have been waiting for regulatory clarity to fund digital currency start-ups. As regulations develop, it will be essential for the digital currency community to have an integral role.

Regulators are not only struggling with how to enforce rules on currencies that do not have a legal jurisdiction or are sponsored by a sovereign government but are also trying to understand the technology behind digital currencies and digital assets. The regulations need to be flexible enough to allow for innovation and encourage digital currency developers to stay within a legal jurisdiction. At the same time, the digital currency space is ripe for fraud, as there is an information advantage for nefarious developers.

The ideal regulatory environment will be one in which the global digital currency community agrees on a set of rules that define good practices. These good practices should be adopted by all white-hatted developers and should be demanded by digital currency users. It is important for the digital currency community to recognize it is better to work with regulators than to push against them. The self-regulatory agencies that already exist in the financial markets can be used as template for digital currencies.

The next stage of growth for digital currencies will involve acceptance by the general public, which makes it imperative that a set of good practices are adopted. The blockchain technology is revolutionary and can be used for more application than simple value transfer. It is too important a development to be usurped by ne'er-do-wells. The Internet began as a way to send files between computers and has flourished into a technology that allows doctors to remotely perform lifesaving surgeries. The potential for the blockchain is as large as the Internet. With the regulatory picture in focus, the journey into adulthood for digital currencies can begin.

Chapter 11

Smart Money: Set It and Forget It

> I think the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but that will soon be developed is a reliable e-cash.
>
> —Milton Friedman

Ron Popeil made a fortune with a chicken roaster and a phrase: "Set it and forget it!" The Showtime Rotisserie made life easier and solved the problem we all have—not enough time to cook a healthy affordable meal. With his rotisserie and a phrase, Popeil promised that you could make a delicious and healthy meal in two easy steps. Once you prepared the chicken, you simply set the machine in motion and forgot about it until the timer buzzed. You can do something similar with Bitcoin. No, it will not cook a chicken, but you can "set it and forget it." Through the smart money features of Bitcoin, you can literally set up a transaction and forget it—the Bitcoin software does the rest.

But wait, there's more. You can also attach a contract or property to the transaction and the Bitcoin network will verify that you own it and transfer it when you want to whom you want.

As these pages are being written, entrepreneurial coders are hard at work on features called smart contracts and smart property. Smart contracts are legal documents that are attached to a bitcoin transaction. These contracts stipulate who to pay, when to pay, and what is being exchanged—and they are incredibly efficient. Also, since the bitcoin transaction is irreversible and a signed contract is attached, dispute resolution will be dramatically reduced.

Smart property is any piece of property that can be digitally identified. For example, every security in North America can be identified by its Committee on Uniform Securities Identification Procedures (CUSIP) number. This nine-character alphanumeric code is used for settling and transferring securities. Currently, the process of distributing the number is owned by the American Bankers Association and operated by S&P Capital IQ. When a security is transferred between two parties, the CUSIP number identifies the property (share of stock), and the clearinghouse filled with people and computers complete transfer. This entire process can be streamlined by attaching the CUSIP number to a bitcoin transaction. A stock certificate that is transferred via the Bitcoin network is a simple example of smart property.

Smart contracts and property are part of the growing Bitcoin ecosystem that is fortifying the backbone of smart money. This part of the Bitcoin ecosystem is moving so fast that many are referring to the speed of change as "Bitcoin time." However, before we move forward, we must take a trip back in time.

In the olden days—way back in the 1960s—e-mail existed for computer scientists to communicate with each other over specific closed mainframe computers. A decade later the U.S. government's Advanced Research Projects Agency (ARPA, DARPA) decided to interconnect different computer systems and call it ARPANET. For all intents and purposes, the establishment of ARPANET was the birth of the Internet. Now that computer systems were interconnected, the Defense Advanced Research Projects Agency (DARPA) needed a way to communicate across different platforms. The previous e-mail systems were closed to the rest of the Internet because each network spoke a different language and operated under a different set of rules called protocols.

In the early 1970s, the Simple Mail Transfer Protocol (SMTP) was developed and allowed different computer systems to communicate. DARPA's standardized set of rules was similar to the standards accepted for building railroads across the United States. The acceptance of George Stephenson's "Standard Gauge" allowed railcars to travel across country without the need to change tracks. The proliferation of SMTP allowed communication to travel across computer systems.

Money is similar to e-mail—both convey a message and both require a set of rules to transfer that message from one person to another. The message of money is value; by sending money you are transferring value from one person to another. If you buy a shirt for $35, you are sending this message to your bank:

> Dear Bank,
>
> I am currently shopping at Rudy's House of Awesome Shirts and have found a shirt I really like, in fact, it's awesome. This shirt cost $35 and I wish to have this shirt more than I wish to have $35. Please transfer $35 to Rudy's House of Awesome Shirts from my account so that I may leave the store with this awesome shirt in my possession.
>
> Regards,
> Me

Once your bank receives this message, there is a set of rules it follows to make the transfer to Rudy's House of Awesome Shirts. Of course, you never see all this communication because a debit card makes it seem easy, but rest assured there are messages flying through cyberspace making sure you get your awesome shirt.

The current financial system has developed these protocols, or rules, so that different banks could communicate and transfer value. As banks globalized, another set of rules was needed so that the money spoke the same language—that is, the message "Please transfer $35," could be easily translated into other currencies. These protocols govern modern finance, but in the Bitcoin financial system, these rules are just being developed.

Rules of the Road

Today, there are three protocols competing to become the next SMTP. Ripple, MasterCoin, and ColoredCoin are all trying to make value

transfer seamless across computers, currencies, and national borders. Ripple is both a currency and a protocol, and its aim is to make it possible to transfer any type of value across a distributed network. They call it e-mail for money. What makes Ripple unique is that it is competing with Bitcoin as a currency. With Ripple, value can be transferred instantly and for free whether that value is stored in euros, U.S. dollars, bitcoins, or Ripples.

MasterCoin and ColoredCoin are taking a different approach—by using the existing bitcoin network, they are designing products that ride on top. Both ColoredCoin and MasterCoin allow end users to create their very own currency.

Smart Contracts and Property

Once the rules of the road for money are established, we will be able to transfer virtually anything of value. E-mail allowed us to send any message to any person that was connected to the Internet. Because the Bitcoin protocol has solved the problem of transferring secure information over an insecure network, it can be used to send value over the Internet. However, we will need some rules to guide us, but this time they already exist, they just need to be turned into computer code.

In their simplest form, contracts are the set of rules to be followed when two people decide to exchange something of value. The contract you sign when buying a house contains instructions for both the buyer and the seller. When it comes to using contracts in conjunction with Bitcoin, the contracts need to go to school and become smart contracts. Smart contracts are contracts that are embedded into property and turn formerly dumb property in smart property.

Your mobile phone is a great example of a contract embedded in a piece of property, making your phone smart property. In order to verify that the user of the phone is the true owner, your mobile phone works only if you type in the correct personal identification number (PIN)—embedded in the phone software is a contract that states the phone will only operate for the rightful owner. The key to proving you are the rightful owner is your PIN. But you also have a smart contract with your mobile service provider. You have signed a contract with AT&T,

Verizon, or Sprint in which they agreed to provide mobile phone coverage in exchange for a payment. If your payment does not arrive as agreed, your mobile phone is disconnected.

Another real-world example of the smart property/contract concept is an immobilizer for automobile. This electronic device prevents the engine from running unless the correct "key" is present. This key can be a code or PIN or even use cryptography to create a secure encryption. These devices have been mandatory in Germany, the United Kingdom, and Finland since 1998. In Australia, where the immobilizers have been mandatory since 2001, they have reduced auto theft by 45 percent. If the proper token or code is not present then the device does not allow fuel to flow to the engine—in this way it prevents a car from being hotwired after access has been gained.

Since bitcoins can be divided down to eight decimal places, it is feasible that the smallest denomination of bitcoin (a Satoshi) could be embedded in every car that rolls off an assembly line. When the car is transferred to the dealer, that transaction will be recorded in the blockchain, and when you purchase the car, the transfer is also logged in the central ledger. This would create one single record of ownership and could eliminate vehicle identification numbers. Additionally, anyone who subsequently purchased the car would simply be able to look at the blockchain to determine all the owners of the vehicle. Misrepresentation of true ownership by unscrupulous sellers would be eliminated.

The first person to propose the idea of a smart contract was law professor Nick Szabo—yep, that Nick Szabo—the one everybody had once pegged as Satoshi Nakamoto. In 1997, Nick Szabo wrote a paper called "The Idea of Smart Contracts," in which he described contractual clauses digitally embedded into property. In fact, in this paper, not only does he describe the idea of an automobile immobilizer, but he also examines how smart contracts could be used for peer-to-peer lending. Since smart contracts are attached to any collateral that would be lent against if the borrower defaults on the agreement, ownership of the property would simply revert back to the lender.

Bitcoin allows this simple contract process to be embedded in virtually anything that can be digitally identified. The requirement for digital identification is not as ominous as it sounds, it could be as simple as placing a barcode on an object, whether it be an antique lamp or a house. As

long as that barcode cannot be removed from the property, ownership can be transferred using the Bitcoin network. The advantage to using Bitcoin is that the protocol has embedded security and does not require a lawyer to write the contract. This is just another way that Bitcoin could disintermediate a service industry.

These smart contracts can also be used to remove the middleman of the banking system which would be an extension of Nick Szabo's original thesis on peer-to-peer lending. In a typical car loan, the bank loans you money to purchase an automobile, and if the loan is not repaid as scheduled, the bank hires a repo man to take back its collateral. Using the smart contract properties of Bitcoin, the loan agreement could be embedded in your key—if your loan is not repaid according to the agreement, the key will not start the car. Moreover, using GPS the bank could locate the car and send a representative with a new key to drive the vehicle away, no repo man needed.

Of course, with this level of control over collateral, one need not be a bank to make this loan. Individuals with cash to lend have an unprecedented opportunity to securely lend money without a middleman. This is an enormous step forward for peer-to-peer (P2P) lending. The problem with P2P lending is that the lender does not have a reasonable assurance that she can repossess the collateral if the agreement is breached. If somebody does not pay you back now, you must file a legal claim in court. There is a cost associated with not just hiring a lawyer but the time spent documenting the transaction.

To see how this would work, suppose you loan me money to buy a car and we agree that each month I will pay you $300. We write this contract into our Bitcoin transaction and broadcast it to the network to record and verify. Now we have an irreversible digital record of our transaction. We also write into our transaction that if I don't pay you, you have the right to repossess my car. As we saw with the bank example, repossessing collateral is pretty simple with Bitcoin. When my payment does not arrive as agreed, our digital contract shuts my car off and disables the key. As per our contract, ownership is transferred to you and a new key is programmed—you hold this new key and are now the rightful owner of the vehicle. Of course, you still need to find the car, but modern-day positioning technology can help with that.

Looking at the idea of combining smart contracts with automobiles does not need to be an exercise in loan defaults and repossessions.

Imagine that you own a brand new Tesla and that you are taking a business trip to Los Angeles. Let's also assume Tesla has embraced Bitcoin and each new Tesla is embedded with one Satoshi of bitcoin during the manufacturing process. The proof of your ownership will be recorded in the blockchain, but you do not have to transfer complete ownership in order to derive a benefit from the Bitcoin technology. Using a smart contract attached to your Tesla, you could sell usage time in your car, a P2P automobile timesharing service. Instead of renting a car from Hertz or Avis, you could trade the usage of your Tesla in New York for usage of a Tesla in Los Angeles. This could revolutionize the way cars are sold. Dealers may soon be asking, "Would you like the rental option with your purchase?" Not only would this change the way cars are sold; it would also provide a new asset class for Wall Street to trade, package, and resell.

Smart property and contracts could be used in financial services as well. Trust companies, like U.S. Trust and Bank of New York, offer clients a neutral third party who will transfer assets (value) when certain conditions are met—usually the age of 21 or upon death. Typically, an individual wishing to transfer generational wealth would enlist an attorney to draw up the trust documents. Then the assets to be transferred would be placed in the trust of a neutral third party. Once the conditions of the trust document have been met, the third party would transfer the assets. At each of the junctures, both the grantor and the beneficiary are charged fees. Using a smart contract with a timestamp, the exact same transaction could take place for virtually no fee.

An attorney may be needed to originally write the trust documents, but once it is coded into a bitcoin, the transaction is on autopilot. The trust document will be recorded in the blockchain with a series of if-then statements. For example, if the beneficiary turns 21 years old, then she receives 100 bitcoins. When the clock strikes midnight on her birthday, the ownership is automatically transferred—the original owner of the bitcoins literally set it and forgot it.

Ethereum

Taking this concept to the next level is the team at Ethereum. Lead Vitalik Buterin, Ethereum is developing a blockchain and programming

language that will allow anyone to build a smart contract application. Ethereum has been called Bitcoin 2.0, but that is a misnomer; bitcoin has clearly gone down the path of a medium of exchange. It is on its way to becoming another global currency. However, Ethereum is attempting to become the "app store" of the digital currency world. Their goal is to develop the computer language that will be the backbone of smart contracts and property apps. Even more, they have established themselves as a nonprofit and plan to give this revolutionary technology away for free.

Before we dig into what Ethereum is, we need to know who Ethereum is. Why is this nonprofit about to change the world? The cofounder and figurehead of the organization is Vitalik Buterin a 20-ish computer scientist who also founded *Bitcoin Magazine*. Buterin is one of the young guns in the digital currency world, where he also has worked on projects like Dark Wallet, a Bitcoin wallet that aims to add another layer of anonymity to the Bitcoin economy. He has also just been awarded a Thiel Fellowship, which provides $100,000 to 20 of the most promising developers in the world. If the name Thiel rings a bell it's because the foundation was setup up by Peter Thiel, the founder of PayPal, early investor in Facebook and big venture capitalist supporting Bitcoin projects.

Along with Vitalik Buterin, the founding team is stacked with an all-star list of computer scientists, cryptographers, and digital currency experts. The one name that sticks out is Ralph Merkle, who is an adviser to Ethereum. Who is Ralph Merkel? He is the person who invented cryptographic hash functions. The complicated mathematical equation that encrypts and secures the Bitcoin network is based on an invention that Ralph Merkle developed for an undergraduate project. He is also one of the inventors of public key cryptography and now is a nanotechnology researcher. If your building an application platform based on the blockchain technology and cryptography, Ralph Merkle is a guy you want to have on your team.

As the price of bitcoin climbed much of the attention has focused using bitcoin as a currency. The concept of a blockchain has found a successful home as a way to securely transfer value over the Internet. However, using the blockchain technology to create a medium of exchange is only one use—it's like using electricity only to power a lamp. The blockchain concept can be used for applications beyond

just money, for example, it can be used to establish and store the ownership of any physical asset that has a digital signature (smart property). The blockchain technology can also be used to transfer these assets using smart contracts with predetermined rules of ownership transfer. A logical extension of this concept is to use the blockchain technology to create and trade financial derivatives like certificates for difference. Additionally, the technology is being used to create decentralized exchanges that will facilitate the transfer of ownership, store the transaction, and act as a decentralized clearinghouse.

As these types of applications are developed there are two important hurdles to overcome—first, Bitcoin is limited in scalability, and second, there needs to be a common language. We have already discussed the transaction limitations of Bitcoin, but there is also an issue of storage. Recall that to keep the Bitcoin network securely running it relies on miners downloading every transaction that has ever taken place. As more transactions are added to the blockchain, the more data needs to be stored on every miner's computer. The strength of a decentralized distributed network is that any node on the network stores the information, and if one node fails, the other nodes continue to function without a hiccup. However, as the blockchain grows, the economic reality of storing all the data means that only miners with the financial ability to store the data in massive databases will be able to act a full node.

Bitcoin has already reached the point where only a few large corporations can afford to mine profitably. These large mining operations are essential to the functioning of the network, but the fact that profitable mining requires a significant financial investment means that the network is becoming more centralized. It is in fact trending toward the financial system we already have, where large commercial banks are essential to the functioning of the system. The largest mining pool already processes close to 50 percent of the transactions on the network; this is almost as far as the network can get from Satoshi's original concept of a decentralized financial system.

The trend toward centralization of the miners is occurring when the network is processing and storing only financial transactions. When other applications of the blockchain technology are developed and deployed the problem will be exacerbated. Miners will no longer be processing purchases at Overstock, they will also be processing and

storing financial derivative contracts, prediction markets, and voting results. In short the larger the Bitcoin network grows the more centralized it will become.

Ethereum is trying to solve this problem by creating an entirely new blockchain that is specifically designed to handle decentralized applications. Ethereum is not trying to compete with Bitcoin, it is simply being developed to fulfill the promise of blockchain concept. Ethereum is tackling the problem of mining centralization by choosing a mining algorithm that will allow any computer to process transactions on the network. In digital currency–speak, this is called an ASIC-resistant algorithm. This means that the algorithm Ethereum uses will not give an advantage to those miners with the most expensive computer. This in itself could be revolutionary in the digital currency world, as it would reverse the trend toward centralization.

The second problem Ethereum is tackling is that of standardization, particularly in the computer language that is used to develop new applications. An easy way to think about this is the difference between Google's Android operating system and Apple's iOS; both can be used to develop apps, but an entirely new app must be written in both languages in order for it to function on either system. Ethereum is developing a language called EVM, which stands for Ethereum Virtual Machine code. EVM will allow anyone to create a decentralized application using any computer language they choose. Once the application is completed, EVM will standardize the code so that it functions smoothly on the Ethereum network.

The goal of Ethereum is to make it possible for any developer to write a smart contract that will operate on the Ethereum blockchain. Once again, the impact of this technology should not be underestimated. The ability to create and distribute decentralized applications has the potential to disrupt a wide swath of businesses, not just in the financial industry.

The Ethereum group imagines three types of applications that will utilize the blockchain: financial applications, semifinancial applications, and nonmonetary applications. The financial applications are the most straightforward since they already exist in another form. An options contract is an example of a prime candidate for decentralization via Ethereum.

A financial option contract gives the buyer the right, not the obligation, to buy or sell a security at a predetermined price. Essentially, it is a contract between buyer and seller that states that on June 30 (expiration date) the buyer of a call option has the right to buy XYZ stock at $75, and the seller of the call option has the obligation to sell XYZ stock at $75. Under the current system, the contract is settled on expiration by the Options Clearing Corporation—a centralized clearinghouse. If the price of XYZ stock is $80 on June 30, then the buyer of the call option will exercise her right to buy XYZ at $75. The Options Clearing Corporation makes sure the seller of the option delivers XYZ stock at $75.

Using Ethereum and the blockchain, the contract between buyer and seller of the option can be programmed and stored in the database that is known as the blockchain. Both the buyer and the seller set aside funds in escrow to settle the transaction, if at expiration XYZ stock is $80, then the Ethereum blockchain automatically transfer ownership of XYZ from the seller to the buyer and credits the buyers account with the $5 difference between the agreed-upon price $75 and the current price $80. This can be accomplished with only a few lines of computer code, removing the Options Clearing Corporation and many other intermediaries in the clearing business. It's fast, it's efficient, and it is being offered for free.

The semifinancial type of application involves a prize or bounty for computational work. For example, the current SETI projects are candidates for decentralization using Ethereum. The Search for Extraterrestrial Intelligence (SETI) is the name for a collection of projects looking for life in outer space. The most famous is SETI@Home run by the University of California–Berkeley. Under this project, any individual can help process the data collected by volunteering use of their home computer for computational purposes. The SETI@Home projects sends "work units" to the computers that have volunteered, and when processing is complete, the results are sent back to the University of California–Berkley. While this project is already a distributed computing project it relies on volunteers. Using Ethereum, the SETI@Home project could offer bounties or make micropayments for computational resources. In this way the transaction is financial, but the result could benefit society as a while (or harm, depending on your opinion of ET).

Finally, the nonmonetary applications can involve voting applications or predication markets. These prediction markets could be used for governing, disrupting the representative political systems that govern most of the world. Let's suppose a town would like to build a new park and has allocated $100,000 from the town budget to complete this work. However, before the work can be done, it must be approved by the citizens. Using EVM, the town could distribute tokens to every citizen and then setup a YES address and a NO address. The citizens would then cast their vote by sending the token to the YES or NO address. This information would be processed, secured, and stored by the Ethereum blockchain. At the end of the predetermined voting time, the town would simply look at which wallet had more tokens; if YES had more tokens, then the park would get built. This would immediately eliminate any vote tampering since the supply of tokens would be fixed, thus any additional tokens would be known to be fraudulent.

Cryptoequities: A New Type of Investment

The ability to attach a contract to a digital currency transaction opens up the possibility that a new asset class may have been born. When an investor buys a bond, she is entering into a contractual agreement with the issuing company to lend money at a predetermined rate. Furthermore, when the investor buys a stock, she is entitled to a piece of the profits proportional to her investment. Both of these contractual agreements can be accomplished easily using smart contracts. Interestingly, this new assets class can be created without the use of an investment bank or other financial intermediaries.

These cryptoequities and cryptobonds are really a hybrid of the traditional stock and bond crossed with a currency. They function like a stock or bond in that they give the holder a claim on certain cash flows, but at the same time they can be used as a medium of exchange. For example, if Ford created a FordCoin, it could use a smart contract to entitle the holder to a portion of the earnings just like Ford stock. The holder of the FordCoin could also use the currency to purchase a new vehicle. When Ford received the FordCoin, it could convert it immediately to fiat currency or it could hold it as an investment. If Ford decided

to hold the coin for investment, it would be similar to a stock buyback, where the coin would be held in the Ford treasury, never to be released to the public markets. Removing the supply from the market should have a positive effect on the price, which may enable more of Ford's customers holding FordCoins to buy a car.

Alternatively, these cryptoequities could be used just like traditional initial public offerings. A company wishing to raise capital could premine a portion of the coin like we did with Nautiluscoin and use the profits from selling the premined coins as capital to operate the business. Once again, this can be accomplished without an investment bank and without regulation. That being said, regulation is likely to become part of the alternative currency ecosystem, but in the beginning it is trending toward being less onerous than traditional securities laws.

The issue that regulators must confront is that alternative currencies are not legal entities and the holders of the coins are not part of the management team. This makes enforcing regulations virtually impossible. Moreover, digital currencies are not domiciled in any particular country, which means they do not fall under any legal system. How and where to regulate digital currencies is the biggest challenge faced by governments and regulatory agencies.

Decentralized Autonomous Organizations

Taking the concept to the next level is the notion of a decentralized autonomous organization, DAO for short. A DAO is a group of like-minded people that gather together to complete a predetermined task. These are virtual entities that replicate the function of a corporation without the legal structure. A DAO consists of members who each have a certain number of shares in the organization. The members of the DAO have the right to spend the organization's resources to accomplish the predetermined task. This can be accomplished using the voting system described for the town park, or it can be preprogrammed during the creation of the DAO.

The resources of the DAO can be monetary or something physical, like computational power. In fact, just like a legal corporation, the types of resources are limitless. One monetary use of a DAO could be

providing insurance for a group that may not be eligible. At its core, an insurance company functions as a pool of money—it collects money from its members, invests the money, and pays out claims from the pool. Suppose there was a group that could not get insurance. They could form a DAO and each deposit a predetermined amount. The DAO would then be instructed by the computer code to invest the money in government bonds and pay the interest received to the shareholders of the DAO. Furthermore, the computer code of the DAO could be configured to pay out insurance claims. This would not only eliminate insurance companies but protect groups that were previously uninsurable.

I feel as though I continue to write the same phrase: the implications of this technology (DAO in this case) cannot be understated. DAOs and blockchain technology need not completely eliminate corporations, but they can be used to make them more efficient. Organization structures can be made flatter, consensus decisions can be reached without endless e-mails and office politics, and resources may be allocated more powerfully.

Professor Money

The concept of smart money has wide-ranging implications from the disruption of the legal profession and banking to the rethinking of corporate organizational structures. The decentralized nature of Bitcoin is being extrapolated to redefine the tried and true tenets of business. Profit maximization is yielding to resource maximization and digital currencies are fueling this change.

At the same time that digital currencies are emerging, the sharing economy is flourishing and the concept of the blockchain is the ideal technology to fuel this new business paradigm. Businesses will need to reexamine profit maximization as a driver of value because with digital currencies, value can be derived through the maximization of resources. It is a new way of looking at business that must be embraced by the next generation of leaders.

Chapter 12

Everything You Know about Business Is Wrong

I have seen the future and it works.

—Lincoln Steffans

Everything you learned about business is wrong. This statement is shocking, true, and is meant to convey the stunning developments that the decentralized distributed Bitcoin network is spawning. The Bitcoin Big Bang is not anarchistic revolt toward a socialistic economic system; it is, in fact, a restorative for capitalism and democracy. Decentralization places the economic power into the hands of the citizens and removes many of the regulations that prevent capitalism from functioning efficiently. Bitcoin, alternative currencies, and the blockchain are the tools that can be used to extract the positive influences of capitalism. These tools can be used to build new businesses or replace broken currency regimes. Moreover, the blockchain concept can be used in applications beyond economics.

First-year business students learn that corporations exist to make a profit. What is missed is the implied "hope" that lies within the profit motive. Corporations were conceived to pool the risk of long overseas voyages and to protect the investors from personal loss beyond the original investment. While these entities are fueled by the profit motive, their continued existence is wholly dependent on whether society values its products. Value is derived from the function of the end product. In the end, any product that does not aid human survival is a luxury good. The implied hope is that a corporation will provide a good or service that adds to the evolution of the human ecosystem.

Determining whether a product or service adds to the human ecosystem is easier than it looks—one need only view the demand for the product. A product that is in high demand by definition adds to human development. The iPhone may have initially looked like a luxury good, but it is now being used to monitor health and for personal safety. The energy used to mine bitcoins may appear to be wasted, but bitcoin is being used to serve the underbanked, eliminate identity theft, and rebuild the financial system. A corporation may overtly look like a profit-sucking vampire squid, but its true purpose is to solve a problem. At its core, a corporation is simply a group of people who agree to work together toward one common goal. This goal could be to find the cure for cancer or to make money in the stock market. If this group fails at its task or its stated goal is no longer valued by society, the business fails.

The modern-day corporation is a centralized labyrinth of organizational structures—vice presidents oversee employees, while senior vice presidents supervise vice presidents, and the CEO is in charge of everything. Additionally, these organizations are divided into different networks, each with its own specific task like accounting, sales, marketing, and distribution. As the organization grows, the structure becomes more complex. The solution to this complexity has been centralization; one person—a traffic cop, if you will—directs each division. The flaw in this structure is that it creates a single point of failure. If the CEO or manager fails to do their job—or, worse, is negligent or unscrupulous—then the entire systems fails.

The annals of business history are replete with cautionary tales of single points of failure. From Enron to Bernie Madoff, when one point in the network controls the entire organization, failure is only a criminal

thought away. But do we need this complexity? What if "corporations" or groups of people could spontaneously convene and agree to solve a problem—how would that work? In fact, there is historical precedent for "spontaneous" corporations. During the sixteenth century, entities were formed for single voyages during the salad days of the spice trade. When the ship returned from the journey, the entity was dissolved and the profits split among the shareholders. Prior to the formation of the Dutch East India Company, the first multinational organization, the business world was a decentralized system consisting of nodes that were spontaneously formed to complete a task—the voyage. The Dutch East India Company changed the way business was conducted, as it was designed to survive multiple voyages and operate across the globe. In short, it ushered in the era of the global multinational corporation.

The Bitcoin Big Bang is another moment in time where the world of business as we know it is about to change. For 400 years, the pendulum has swung toward global multinational business organizations. The three largest corporations in the world by market capitalization are Apple, Exxon, Mobil, and Microsoft; they operate in every country in the world and have over $1 trillion in market capitalization. Together, these three corporations produce more revenue than 87 percent of the world's economies and would rank about 30th on the list of gross domestic product by country. The era of the multinational organization may have swung to an extreme.

Moving back toward the single-voyage decentralized economic system is the promise of Bitcoin. The modern-day equivalent of the single-voyage corporations is the decentralized autonomous organization (DAO). The DAO is exactly the type of organization that comes into existence when a group convenes to accomplish a task. Using the blockchain concept and smart contracts, these individuals can assign value to a task and transfer the outcome (value) of that task to anyone, instantaneously and for free. However, there is a major difference between DAOs and single-voyage corporations of the sixteenth century—these "corporations" are not owned by anyone and exist only by virtue of the task at hand. There is not a CEO, vice president, or manager—in short, there is not a single point of failure.

At this point, you may scoff and retort that in a capitalist system the group would have no motivation without the promise of profits, and

therefore a decentralized autonomous organization would never work. Well, they already do.

Bitcoin miners join together in pools and share computing power with the goal of solving mathematical equations. The bitcoin network depends on these miners to verify that bitcoins are not double spent. For their effort, the miners are rewarded with bitcoins. These mining pools split the profits among the members in proportion to the resources committed. The organizations do not have a CEO, are not registered with any government, and have no payroll—but they do exist.

The profit motive still exists in DAOs, but the concept of the blockchain and the coin reward for mining create a self-contained profit engine. As long as the miners have an ecosystem to turn the reward coins into goods and services, then the entity can continue to fuel the work needed to complete the task. The four pillars on which a digital currency economy depends are the blockchain, mining rewards, merchants, and exchanges. The blockchain is the value transfer mechanism, while the mining rewards provide the profit in the form of freshly minted coins. However, these coins have no value unless merchants accept them or speculators are willing to buy them.

It is essential for all four parts of the digital currency economy to be functioning smoothly as they collectively represent the engine of the system. Each piece is needed to create the self-sustaining profit motive at the heart of the digital ecosystem. These four pillars are like the instruments in an orchestra—separately, their parts may sound disjointed, but when they work together, they produce a symphony. This also makes a digital currency economy more collective in that a community is needed for it to thrive. Collaboration, sharing, and the meshing of resources are all hallmarks of the digital economy, or cryptonomics.

Cryptonomics

Cryptonomics is the study and analysis of the digital currency economy. As we have seen, the digital economy requires a collaborative effort to exist and can differ from traditional economics in the concept of the profit motive. In traditional economics the profit motive is simple to determine—one simply needs to ask if consumers will purchase the end

product at a price above production costs. If the answer is yes, then production commences and the corporate organism comes to life. Marketing, design, manufacturing, and sales all work toward making a profit, gaining market share, and ensuring the corporation is an ongoing entity.

However, in cryptonomics, the end product may not be something that is offered for sale; it may be societal good that is given away for free. This is similar to how Google conducts business. It produces a good and gives it away for free and then profits from the value created. For example, Google's mobile operating system is open source and free, yet Google uses the data it collects from powering more than 50 percent of the world's mobile phones to sell advertisements. Google's profit is at least one step removed from its product. This occurs in cryptonomics—the profit is detached from the financial success of the end product; profit is a function of the interplay among miners, merchants, and exchanges.

Separating the profit from the financial viability of the end product is a radical change in capitalism, but is not unprecedented. Open-source software and the collaborative economy are the roots from which cryptonomics has grown. The typical decision-making process for a profit seeking entity starts with an analysis of the end market, then profit seeking entities need to know how much product to make, at what price to sell it, and how to maintain competitiveness in order to determine if resources should be allocated. However, in cryptonomics, the decision-making process is reversed—the entity begins with the profit and then decides what to produce.

Nautiluscoin is a perfect example of the cryptoeconomic decision-making process. Within the first 60 days of existence, we were able to create an "entity" that had a market capitalization of $1 million without producing a single product. Nautiluscoin does not make a profit; it does not have an organizational chart, it does not have a payroll, it does not have headquarters, and it is not a legal entity. However, alternative currency investors bought the coin and bid up the price creating $1 million in value in 60 days. Now that the value has been created we can make a decision about what to produce—which, of course, is completely reversed from traditional economics. Some coins decide to use the profit to bring water to those who need it, while others may decide to fund cancer research. Another option is to use the profits to fund another business that may have a profitable product but needs seed

capital. Transferring capital from those who have it to those who need it is the essence of capitalism. Bitcoin and alternative currencies provide the path to return the capitalistic economic system to its foundation.

Projects and products funded through alternative currencies have a profit motive, but it is separate from the end result. Moreover, alternative currencies and DAOs can accomplish goals without a corporate structure whose sole purpose is to ensure profitability and sustainability. If an organization can exist to complete a task and does not have corporate structure, then the concept of a profit motive is radically altered.

The idea of the profit motive comes from the rational choice theory, which posits individuals tend to pursue their own self-interests. This is the backbone of free-market capitalism and has driven the global economy for centuries, for better or worse. This is also a theory that I have built my businesses upon. The so-called "eat what you kill" business model fuels much of Wall Street, and it is why Wall Street is more a collection of entrepreneurs than an oligopoly of large financial institutions.

Since the financial crisis of 2008, Wall Street firms have failed to illustrate to Main Street that much of the compensation for financial market participants is in the form of a performance bonus. If a trader at a major Wall Street bank does not perform, she does not get paid. Additionally, if the entire bank does not perform, the bonus pool is cut. Unfortunately, too much attention has been focused on a few bad actors. All systems have flaws, and the financial crisis of 2008 shined a harsh light on the flaws in the free-market capitalist system—but, as they say, sunlight is the best disinfectant.

If the concept of the profit motive is flawed, can corporations or an organization exist to serve the needs of people? The flaw in the profit motive is that it assumes if a business is not profitable, then it is not valued by society. Of course, plenty of things are valued by society but are not profitable—emergency services and public roadways are two extremely valuable "businesses" that are not profitable. There have been some attempts to privatize roadways, but in general these attempts have failed to produce spectacular results.

The development of digital currencies, or cryptocurrencies, holds the potential to develop a new type of economic system. The evolution begins with a decentralized financial system where the players at the

center are disintermediated. Removing the friction from the gears of the financial system allows new entities to operate smoothly and new socioeconomic systems to sprout. Cryptonomics smashes together the concepts of the profit motive, collaborative effort, and societal goods. Digital currencies can spawn microeconomies where public goods may indeed turn a profit. DAOs are the transformational catalyst—the goal of a DAO may be to turn a profit, or it may be to accomplish a goal that is important to a subset of society. The distinguishing factor of a DAO is that it does not a have a corporate structure to fund. That is to say, salaries do not need to be paid, health care costs are zero, and infrastructure costs are born by the shareholders of the DAO. Eliminating most of the organizational costs can make many unprofitable endeavors profitable and could potentially change the way business is structured and analyzed.

The Boston Consulting Group, founded by Bruce Henderson, is one of the Big Three business consulting firms and is famous for three structures they developed to help businesses become more profitable and competitive. The Growth Share Matrix, the Experience Curve Effects, and the Advantage Matrix are in every consultant's tool box. While Michael Porter's Three Generic Strategies have guided many executives' decision-making process. However, the reverse decision-making process of cryptonomics may render them irrelevant.

Growth Share Matrix

Bruce Henderson not only made a fortune by founding the Boston Consulting Group, but he also helped others make fortunes through his keen sense of business dynamics. Henderson has created a vast array of structures to help executives conceptualize each part of their business and analyze profitability. The most famous of the structures is the Growth Share Matrix, also known as the BCG Matrix or the Boston Matrix. The Growth Share Matrix consists of four quadrants named cash cows, dogs, question marks, and stars, as shown in Figure 12.1.

The axes of the matrix are labeled Market Growth and Relative Market Share. The stars reside in the quadrant that has high market growth, and the business has high market share. The question marks are business lines with high market growth, but for some reason the

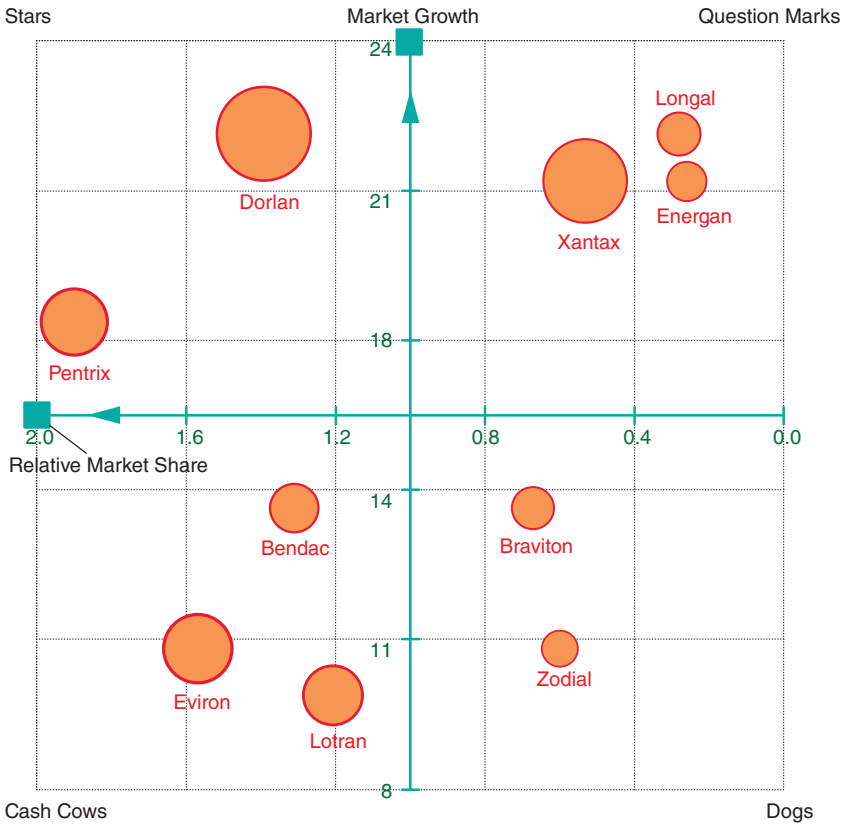

Figure 12.1 The Growth Share Matrix

corporation does not have a large market share. Dogs are business lines that have low market growth, and the corporation has a small market share. Finally, the cash cows are business lines that have slow-growing markets, but the corporation has a high market share and thus enjoys healthy profits.

The entire matrix is designed to help businesses allocate resources to the most profitable businesses. Cash cows are to be milked as long as possible, while dogs are meant to be discarded (sorry, dog lovers). The question marks deserve attention only if the organization believes it can gain market share and become more profitable. Finally, most of a corporation's resources are supposed to be allocated toward the stars, also known as the most profitable businesses.

Cryptonomics renders this matrix irrelevant for the simple fact that its underlying premise is that corporations exist to make a profit. In the cryptoeconomy, organizations exist to complete a task deemed valuable by the stakeholders in the DAO. This may be to turn a profit, or it may be to bring fresh water to a village. Moreover, flattening the organizational structure could realign expenses in such a way that the dogs become a profitable venture. Perhaps it is true that every dog has his day.

Learning Curve Effects

The learning curve was first proposed and observed during experiments on humans memorizing numbers. As the subjects became more adept at memorizing, they could memorize more numbers faster. This concept was then reformulated into the experience curve effect in 1936 at Wright Air Force Base, where it was observed that as aircraft production doubled, it took 10 to 15 percent less labor to produce the one aircraft. The aircraft mechanics were learning from experience and applying that to their work and becoming more efficient.

Once again, Bruce Henderson of BCG formalized the learning curve into the Experience Curve. His early work used the example of the production of the Ford Model T from 1906 to 1916. See Figure 12.2.

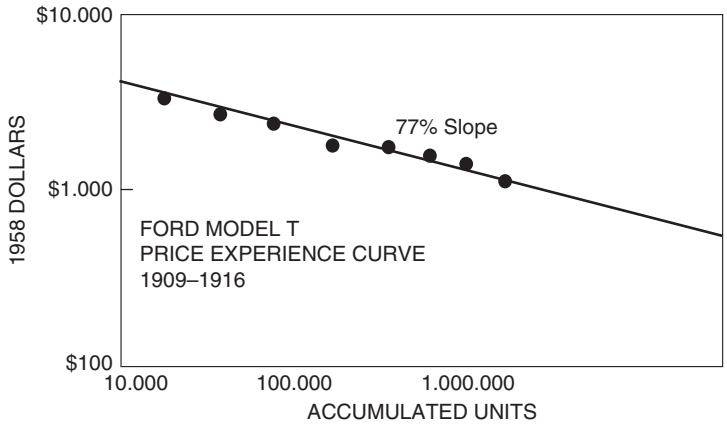

Figure 12.2 Ford Model T Price Experience Curve: 1909–1916

Henderson observed that the cost to produce the Model T dropped as the unit volume increased. While his original work illustrated a linear relationship, he later modified the Experience Curve to include a power law function. That is, as production increased, the cost dropped at an ever-increasing rate.

BCG used this Experience Curve to advise clients to maximize production, as it would drive down costs and increase profits. The bedrock of this observation is that the entity is designed to be ongoing. In the case of a corporation, this is a valid assumption, as incorporation is indefinite. However, in the cryptoeconomy, DAOs can spontaneously organize to complete a task, sometimes for profit and sometimes for social benefit. Since the goal of the DAO is finite, there is not an assumption of an ongoing entity and therefore few repetitive tasks to gain experience. This is not to say that the Experience Curve is invalid; it is just not a useful tool in cryptonomics.

Porter's Three Generic Strategies

Michael Porter has written 18 books on business strategy. He is a renowned professor of strategy and competitiveness at Harvard University, and he is generally considered *the* authority on all things business strategy. He is best known for his Three Generic Strategies, which in simple terms describe how a business can gain a competitive advantage, as shown in Figure 12.3.

His matrix describes three basic ways for a business to compete: differentiation, cost leadership, and strategic focus. If a corporation differentiates its product from others in the marketplace, then consumers may be persuaded to buy more of this product, and more sales means more profit. Once again, the assumptions may be valid in a profit-maximizing world, but in cryptonomics, the goal of the organization may not be profit maximization. Additionally, focusing on a niche market or reducing costs may indeed allow a corporation to become the dominate players in the industry. However, this assumes that both the industry and the corporation will be ongoing.

Cryptonomics does not necessarily make the ongoing concern assumption. A DAO may indeed have an unlimited life span, but it is

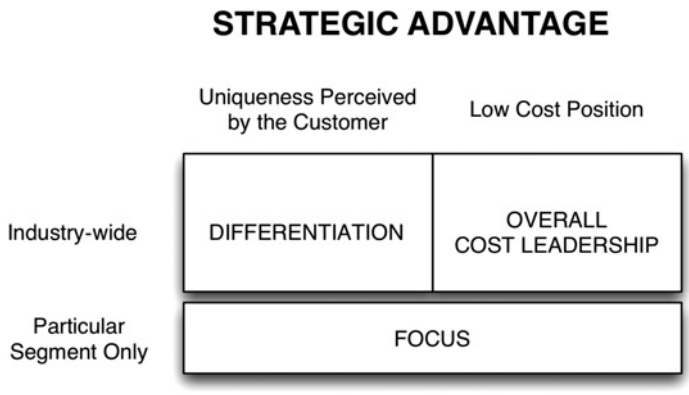

Figure 12.3 Three Generic Strategies

just as likely to fold up shop once its task is completed or profit is made. In this case, there is little need to be the market leader or gain a competitive advantage since the market may disappear as a direct result of the DAO's solving a problem.

Human Resource Management

The Society for Human Resource Management (SHRM) was founded in 1948 and has grown to be the world's largest human resource trade organization. SHRM has 275,000 members in 160 countries—I mention this not because I like writing statistics, but because blockchain technology and DAOs have the potential to disrupt this entire group. Human resource management is charged with making sure employees are paid and treated fairly and generally provides a healthy workplace. But with a DAO there are no employees; every stakeholder in the DAO is an independent contractor. Without humans there is little need to manage those resources.

Alternatively, there may be a need to integrate DAOs with traditional corporations. The trend in business is already to hire as many independent contractors as possible to reduce ancillary costs. If a corporation can engage a DAO to solve a problem, then that business relationship would need to be integrated into the current organizational structure.

Disruption does not always have to mean industries are destroyed—it can also mean they evolve.

Fueling the Sharing Economy

Since the financial crisis of 2008, another economic evolution that has occurred is the rise of the so-called sharing economy. The sharing economy goes by many monikers, including the peer-to-peer economy, the mesh economy, and collaborative consumption, all of which describe an economic system that shares human and physical assets. The backbone of the sharing economy is the premise that when resources are shared, they not only can be allocated more efficiently but they can also gain value by more people and businesses having access. The driving tenet is that unused resources are wasted value.

The concept of the sharing economy gained popularity during the early 2000s when open-source software became increasingly prevalent. The sharing economy seeks to solve the problem of the tragedy of commons, which plagues the free-market economic model—that is, when we all act in our own self-interest, we tend to deplete and waste resources. It is beyond the scope of this book to delve into whether the self-interested profit motive is responsible for the flaws in capitalism, but what is important is that alternative currencies have added a profit engine to the sharing economy. Alternative currencies allow the self-interested profit motive to fuel the sharing economy.

Some of the successful early sharing businesses have used a rental/lease business model. For example, both ZipCar and AirBnB provide a platform to rent/lease unused vehicle hours and apartments. This model works because the resources are easily shared and those using the service get utility out of the product—that is, the ZipCar user gets from point A to point B and the AirBnB customer has a place to rest his head. However, when the utility is less apparent, the model has counted on the kindness of strangers as Kickstarter does.

For those unfamiliar, Kickstarter is the world's largest crowdsourcing platform for creative projects. The creative projects funded have less obvious or broad utility and are thus limited to funding by only true enthusiasts. This type of microfunding is a revolution in its own right,

but it is only scalable to the extent that there are enough donors to support these micro ecosystems. One still runs into the problem of tying the profits or "utility" to the end product. Alternative currencies have the potential to change this dynamic.

If we think about a Kickstarter campaign as a DAO, then we can apply all the benefits of cryptonomics to the project. Let's suppose a community spontaneously forms an organization with the goal of producing a documentary film, and to fund the film they turn to a crowdfunding platform like Kickstarter. A successful fundraising campaign requires a minimum number of interested parties with money to donate in order to support the project. However, with alternative currencies, the "donors" do not have to have a personal interest in the project at all.

If the DAO creates a currency to support the project and uses smart contracts to distribute future earnings from the documentary, it will broaden its capital-raising potential. Those who buy the alternative currency will receive a portion of the cash flow from the film and have the potential for capital appreciation of the digital currency. In this way, alternative currencies smash together the positive motivational aspect of profits with altruistic motives of supporting a creative project. However, this is not just a way for currency speculators to feel good about themselves; it is actually an improvement on the capitalist system.

Capitalism is the best system humans have developed to efficiently allocate resources, until now. The mere fact that there are unused resources to share is evidence that capitalism is not functioning as efficiently as it can. The sharing economy sought to solve this wasted resource problem, and with the addition of alternative currencies this new socioeconomic system can tap into the primal human emotion of greed.

In Oliver Stone's classic movie *Wall Street,* the main villain is Gordon Gekko—he is revered for his cutthroat self-interested business model. In a seminal speech, oft repeated by up-and-coming Wall Street titans, Gordon Gekko expounds on the virtue of greed.

> The point is, ladies and gentleman, that greed—for lack of a better word—is good.
>
> Greed is right.
>
> Greed works.

> Greed clarifies, cuts through, and captures the essence of the evolutionary spirit.
>
> Greed, in all of its forms—greed for life, for money, for love, knowledge—has marked the upward surge of mankind.

While the movie was ostensibly about the greed for money, there is a lesson that the sharing economy can take from Gordon Gekko. Whether we like it or not, greed is a tremendous motivator. The development of alternative currencies along with the interplay of the sharing economy and speculators has created an environment where greed and altruism can exist together. In fact, they not only can exist but they can thrive.

The Future Just Might Work

Lincoln Steffens was a turn-of-the-twentieth-century muckraker who advocated political revolution over reform. His views were no doubt controversial, especially when he returned from a three-week visit to the Soviet Union in 1919. Steffens reportedly called Soviet Russia "a revolutionary government with an evolutionary plan." His enthusiasm for the Soviet revolution resulted in his oft-quoted phrase "I have seen the future, and it works." He believed that the Soviet Revolution was about to change the world and that through collaboration and sharing of resources the future would work better. However, by the time of his death in 1936, he was no longer so enthusiastic about the October Revolution.

The major change in the Soviet Union since Steffen's visit was Lenin's death and Joseph Stalin's appointment as General Secretary of the Central Committee. The development that is important to Bitcoin and the cryptoeconomy is that with this appointment there became a single point of failure. The atrocities committed by Stalin had nothing to do with the particular economic system chosen. A nefarious central government can commit crimes against humanity under capitalism, communism, or any other system. The centralization of political and financial power is the weakest link.

The key to the success of any economic system is a political structure that is flexible enough to govern efficiently and decentralizes power to the citizens. Democracy is essential for capitalism to fulfill its promise of

efficiently allocating resources to serve the needs of society. Without the ability to correct excesses, any system can be hijacked by the politically and financially powerful. The concept of a transparent system that allows the stakeholders to trust each other without knowing each other is a major step forward in the evolution of economic and political systems.

The idea of a transparent blockchain that can be used to collectively allocate resources, vote, and problem solve is the essence of democracy—one human, one vote. The representative democracies that currently exist were logistically necessary since it was impossible for an entire nation to vote on every single piece of legislation. While we elect representatives to look after our interests this system once again creates a single point of failure and currently skews incentives toward self-interest.

As the decentralized distributed concept of the blockchain moves us back toward the founding concepts of democracy, the economic and political system will become less concentrated. All systems have boundaries beyond which they break; in political and economic systems, that boundary is excessive centralization. Alternative currencies; the blockchain; and the transparent, trustless system they have created have the potential to swing the pendulum back toward a more democratic economic and political system.

The Bitcoin Big Bang is a social and economic revolution that will propel the next surge of human development. It will leverage what we have learned about capitalism and fuse it with collaborative consumption to produce a socioeconomic system that is fueled by the profit motive but serves the needs of society. The financial crisis of 2008 fertilized the ground for economic change. The crisis highlighted our economic warts and pushed the concept of centralization to its breaking point. As the pendulum began to swing back toward a decentralized economic system, Bitcoin emerged on cue. Bitcoin and the blockchain will play a starring role in the new economy. It will liberate and accelerate the rebuilt financial systems, and it will solve problems that we may not know we have. In short, Bitcoin is the right idea at the right time.

To paraphrase Lincoln Steffens, we have seen the future, and it just might work.

Appendix 1

Department of the Treasury Financial Crimes Enforcement Network Guidance

FIN-20 13-G00 1
Issued: March 18, 2013
Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[1] Such persons are referred to in this guidance

[1] FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. See Treasury Order 180–01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.

as "users," "administrators," and "exchangers," all as defined below.[2] A user of virtual currency is **not** an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and record-keeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

Currency vs. Virtual Currency

FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[3] In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

Background

On July 21, 2011, FinCEN published a Final Rule amending definitions and other regulations relating to money services businesses ("MSBs").[4] Among other things, the MSB Rule amends the definitions of dealers in

[2]FinCEN's regulations define "person" as "an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities." 31 CFR § 1010.100(mm).

[3]31 CFR § 1010.100(m).

[4]Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011) (the "MSB Rule"). This defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in

foreign exchange (formerly referred to as "currency dealers and exchangers") and money transmitters. On July 29, 2011, FinCEN published a Final Rule on Definitions and Other Regulations Relating to Prepaid Access (the "Prepaid Access Rule").[5] This guidance explains the regulatory treatment under these definitions of persons engaged in virtual currency transactions.

Definitions of User, Exchanger, and Administrator

This guidance refers to the participants in generic virtual currency arrangements, using the terms "user," "exchanger," and "administrator."[6] A *user* is a person that obtains virtual currency to purchase goods or services.[7] An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

Users of Virtual Currency

A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is **not** an MSB under FinCEN's regulations.[8] Such activity, in and of itself, does not fit within the

---

paragraphs (ff)(1) through (ff)(7) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States." 31 CFR § 1010.100(ff).

[5]Final Rule—Definitions and Other Regulations Relating to Prepaid Access, 76 FR 45403 (July 29, 2011).

[6]These terms are used for the exclusive purpose of this regulatory guidance. Depending on the type and combination of a person's activities, one person may be acting in more than one of these capacities.

[7]How a person engages in "obtaining" a virtual currency may be described using any number of other terms, such as "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing," depending on the details of the specific virtual currency model involved. For purposes of this guidance, the label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the BSA of the process or of the person engaging in the process.

[8]As noted above, this should not be interpreted as a statement about the extent to which the user's activities comport with other federal or state statutes, rules, regulations, or orders. For example, the activity may still be subject to abuse in the form of trade-based money laundering or terrorist financing. The activity may follow the same patterns of behavior observed in the "real" economy with respect

definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.[9]

Administrators and Exchangers of Virtual Currency

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.[10] FinCEN's regulations define the term "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[11]

The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.[12] FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and de-centralized convertible virtual currencies.

---

to the purchase of "real" goods and services, such as systematic over- or under-invoicing or inflated transaction fees or commissions.

[9] 31 CFR § 1010.100(ff)(1–7).

[10] FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)-(F).

[11] 31 CFR § 1010.100(ff)(5)(i)(A).

[12] Ibid.

a. E-Currencies and E-Precious Metals

The first type of activity involves electronic trading in e-currencies or e-precious metals.[13] In 2008, FinCEN issued guidance stating that as long as a broker or dealer in real currency or other commodities accepts and transmits funds solely for the purpose of effecting a *bona fide* purchase or sale of the real currency or other commodities for or with a customer, such person is not acting as a money transmitter under the regulations.[14]

However, if the broker or dealer transfers funds between a customer and a third party that is not part of the currency or commodity transaction, such transmission of funds is no longer a fundamental element of the actual transaction necessary to execute the contract for the purchase or sale of the currency or the other commodity. This scenario is, therefore, money transmission.[15] Examples include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer's account; (2) the transfer of value from a customer's currency or commodity position to the account of another customer; or (3) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party. Since the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies, the same rules apply to brokers and dealers of e-currency and e-precious metals.

---

[13]Typically, this involves the broker or dealer electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency. However, the same conclusions would apply in the case of the broker or dealer issuing paper ownership certificates or manifesting customer ownership or control of real currencies or commodities in an account statement or any other form. These conclusions would also apply in the case of a broker or dealer in commodities other than real currencies or precious metals. A broker or dealer of e-currencies or e-precious metals that engages in money transmission could be either an administrator or exchanger depending on its business model.

[14]Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities, FIN-2008-G008, Sept. 10, 2008. The guidance also notes that the definition of money transmitter excludes any person, such as a futures commission merchant, that is "registered with, and regulated or examined by … the Commodity Futures Trading Commission."

[15]In 2011, FinCEN amended the definition of money transmitter. The 2008 guidance, however, was primarily concerned with the core elements of the definition—accepting and transmitting currency or value—and the exemption for acceptance and transmission integral to another transaction not involving money transmission. The 2011 amendments have not materially changed these aspects of the definition.

b. Centralized Virtual Currencies

The second type of activity involves a convertible virtual currency that has a centralized repository. The administrator of that repository will be a money transmitter to the extent that it allows transfers of value between persons or from one location to another. This conclusion applies, whether the value is denominated in a real currency or a convertible virtual currency. In addition, any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on behalf of others, including transfers intended to pay a third party for virtual goods and services, is also a money transmitter.

FinCEN understands that the exchanger's activities may take one of two forms. The first form involves an exchanger (acting as a "seller" of the convertible virtual currency) that accepts real currency or its equivalent from a user (the "purchaser") and transmits the value of that real currency to fund the user's convertible virtual currency account with the administrator. Under FinCEN's regulations, sending "value that substitutes for currency" to another person or to another location constitutes money transmission, unless a limitation to or exemption from the definition applies.[16] This circumstance constitutes transmission to **another location**, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator. It might be argued that the exchanger is entitled to the exemption from the definition of "money transmitter" for persons involved in the sale of goods or the provision of services. Under such an argument, one might assert that the exchanger is merely providing the service of connecting the user to the administrator and that the transmission of value is integral to this service. However, this exemption does not apply when the only services being provided are money transmission services.[17]

The second form involves a *de facto* sale of convertible virtual currency that is not completely transparent. The exchanger accepts currency or its equivalent from a user and privately credits the user with an

[16]See footnote 11 and adjacent text.
[17]31 CFR § 1010.100(ff)(5)(ii)(F).

appropriate portion of the exchanger's own convertible virtual currency held with the administrator of the repository. The exchanger then transmits that internally credited value to third parties at the user's direction. This constitutes transmission to **another person**, namely each third party to which transmissions are made at the user's direction. To the extent that the convertible virtual currency is generally understood as a substitute for real currencies, transmitting the convertible virtual currency at the direction and for the benefit of the user constitutes money transmission on the part of the exchanger.

c. De-Centralized Virtual Currencies

A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort.

A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.

Providers and Sellers of Prepaid Access

A person's acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies.[18]

[18] This is true even if the person holds the value accepted for a period of time before transmitting some or all of that value at the direction of the person from whom the value was originally accepted. FinCEN's

Dealers in Foreign Exchange

A person must exchange the currency of two or more countries to be considered a dealer in foreign exchange.[19] Virtual currency does not meet the criteria to be considered "currency" under the BSA because it is not legal tender. Therefore, a person who accepts real currency in exchange for virtual currency, or vice versa, is not a dealer in foreign exchange under FinCEN's regulations.

Financial institutions with questions about this guidance or other matters related to compliance with the implementing regulations of the BSA may contact FinCEN's Regulatory Helpline at (800) 949-2732.

---

regulations define "prepaid access" as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number." 31 CFR § 1010.100(ww). Thus, "prepaid access" under FinCEN's regulations is limited to "access to funds or the value of funds." If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency." 31 CFR § 1010.100(ff)(5)(i).

[19] FinCEN defines a "dealer in foreign exchange" as a "person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery." 31 CFR § 1010.100(ff)(1).

Appendix 2

New York State Department of Financial Services Proposed New York Codes, Rules and Regulations

Title 23. Department of Financial Services
Chapter I. Regulations of the Superintendent of Financial Services
Part 200. Virtual Currencies

Section 200.1 Introduction

This Part contains regulations relating to the conduct of business involving Virtual Currency, as defined herein, in accordance with the superintendent's powers pursuant to the above-stated authority.

Section 200.2 Definitions

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that directly or indirectly controls, is controlled by, or is under common control with, another Person;
(b) *Cyber Security Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a Licensee's electronic systems or information stored on such systems;
(c) *Department* means the New York State Department of Financial Services;

(d) *Fiat Currency* means government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law;

(e) *Licensee* means any Person duly licensed by the superintendent pursuant to this Part;

(f) *New York* means the State of New York;

(g) *New York Resident* means any Person that resides, is located, has a place of business, or is conducting business in New York;

(h) *Person* means an individual, partnership, corporation, association, joint stock association, trust, or other business combination or entity, however organized;

(i) *Principal Officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

(j) *Principal Stockholder* means any Person that directly or indirectly owns, controls, or holds with power to vote ten percent or more of any class of outstanding capital stock of a corporate entity or possesses the power to direct or cause the direction of the management or policies of the entity;

(k) *Principal Beneficiary* means any Person entitled to ten percent or more of the benefits of a trust;

(l) *Transmission* means the transfer, by or through a third party, of Virtual Currency from one Person to another Person, including the transfer from the account or storage repository of one Person to the account or storage repository of another Person;

(m) *Virtual Currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort. Virtual Currency shall not be construed to include digital units that are used solely within online gaming platforms with no market

or application outside of those gaming platforms, nor shall Virtual Currency be construed to include digital units that are used exclusively as part of a customer affinity or rewards program, and can be applied solely as payment for purchases with the issuer and/or other designated merchants, but cannot be converted into, or redeemed for, Fiat Currency;

(n) *Virtual Currency Business Activity* means the conduct of any one of the following types of activities involving New York or a New York Resident:

(1) receiving Virtual Currency for transmission or transmitting the same;

(2) securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;

(3) buying and selling Virtual Currency as a customer business;

(4) performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or

(5) controlling, administering, or issuing a Virtual Currency.

Statutory Authority: Financial Services Law, sections 102, 201, 301, and 302

Section 200.3 License

(a) License required. No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity.

(b) Unlicensed agents prohibited. Each Licensee is prohibited from conducting any Virtual Currency Business Activity through an agent or agency arrangement when the agent is not a Licensee.

(c) Exemption from licensing requirements. The following Persons are exempt from the licensing requirements otherwise applicable under this Part:

(1) Persons that are chartered under the New York Banking Law to conduct exchange services and are approved by the superintendent to engage in Virtual Currency Business Activity; and

(2) merchants and consumers that utilize Virtual Currency solely for the purchase or sale of goods or services.

Section 200.4 Application

(a) Application for a license required under this Part shall be in writing, under oath, and in a form prescribed by the superintendent, and shall contain the following:

(1) the exact name of the applicant, including any doing business as (DBA) name, the form of organization, the date of organization, and the jurisdiction where organized or incorporated;

(2) a list of all of the applicant's Affiliates and an organization chart illustrating the relationship among the applicant and such Affiliates;

(3) a list of, and detailed biographical information for, each individual applicant and each director, Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, including such individual's name, physical and mailing addresses, and information and documentation regarding their personal history, experience, and qualification, which shall be accompanied by a form of authority, executed by such individual, to release information to the Department;

(4) a background report prepared by an independent investigatory agency acceptable to the superintendent for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable;

(5) for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and for all individuals to be employed by the applicant: (i) a set of completed fingerprints, or a receipt indicating the vendor (which vendor must be acceptable to the superintendent) at which, and the date when, the fingerprints

were taken, for submission to the State Division of Criminal Justice Services and the Federal Bureau of Investigation; (ii) if applicable, such processing fees as prescribed by the superintendent; and (iii) two portrait-style photographs of the individuals measuring not more than two inches by two inches;

(6) an organization chart of the applicant and its management structure, including its Principal Officers or senior management, indicating lines of authority and the allocation of duties among its Principal Officers or senior management;

(7) a current financial statement for the applicant and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and a projected pro forma balance sheet and income and expense statement for the next year of the applicant's operation;

(8) a description of the proposed, current, and historical business of the applicant, including detail on the products and services provided and to be provided, all associated website addresses, the jurisdictions in which the applicant is engaged in business, the principal place of business, the primary market of operation, the projected customer base, any specific marketing targets, and the physical address of any operation in New York;

(9) details of all banking arrangements;

(10) all written policies and procedures, including those required by this Part;

(11) an affidavit describing any administrative, civil, or criminal action, litigation, or proceeding before any governmental agency, court, or arbitration tribunal and any existing, pending, or threatened action, litigation, or proceeding against the applicant or any of its directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries, as applicable, including the names of the parties, the nature of the proceeding, and the current status of the proceeding;

(12) if applicable, a copy of any insurance policies maintained for the benefit of the applicant, its directors or officers, or its customers;

(13) an explanation of the methodologies used to calculate the value of Virtual Currency in Fiat Currency; and

(14) such other additional information as the superintendent may require.

(b) As part of such application, the applicant shall demonstrate that it will be compliant with all of the requirements of this Part upon licensing.

(c) The superintendent may permit that any application for a license under this Part, or any other submission required by this Part, be made or executed by electronic means.

Section 200.5 Application Fees

As part of an application for licensing under this Part, each applicant must submit an initial application fee, in an amount prescribed by the superintendent, to cover the cost of processing the application, reviewing application materials, and investigating the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the application is denied or withdrawn, such fee shall not be refunded. Each Licensee may be required to pay fees to the Department to process additional applications related to the license.

Statutory Authority: Financial Services Law, sections 202, 206, 301, 302, and 304-a; State Administrative Procedures Act, section 102

Section 200.6 Action by Superintendent

(a) Generally. Upon the filing of an application for licensing under this Part, payment of the required fee, and demonstration by the applicant of its ability to comply with the provisions of this Part, the superintendent shall investigate the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the superintendent finds these qualities are

such as to warrant the belief that the applicant's business will be conducted honestly, fairly, equitably, carefully, and efficiently within the purposes and intent of this Part, and in a manner commanding the confidence and trust of the community, the superintendent shall advise the applicant in writing of his or her approval of the application, and shall issue to the applicant a license to conduct Virtual Currency Business Activity, subject to the provisions of this Part and such other conditions as the superintendent shall deem appropriate; or the superintendent may deny the application.

(b) Approval or denial of application. The superintendent shall approve or deny every application for a license hereunder within 90 days from the filing of an application deemed by the superintendent to be complete. Such period of 90 days may be extended at the discretion of the superintendent for such additional reasonable period of time as may be required to enable compliance with this Part. A license issued pursuant to this Part shall remain in full force and effect until it is surrendered by the Licensee or revoked or suspended as provided in this Part.

(c) Suspension or revocation of license. The superintendent may suspend or revoke a license issued under this Part on any ground on which the superintendent might refuse to issue an original license, for a violation of any provision of this Part, for good cause shown, or for failure of the Licensee to pay a judgment, recovered in any court, within or without this State, by a claimant or creditor in an action arising out of, or relating to, the Licensee's Virtual Currency Business Activity, within thirty days after the judgment becomes final or within thirty days after expiration or termination of a stay of execution thereon; provided, however, that if execution on the judgment is stayed, by court order or operation of law or otherwise, then proceedings to suspend or revoke the license (for failure of the Licensee to pay such judgment) may not be commenced by the superintendent during the time of such stay, and for thirty days thereafter. "Good cause" shall exist when a Licensee has defaulted or is likely to default in performing its obligations or financial engagements or engages in unlawful, dishonest, wrongful, or inequitable conduct or practices that may cause harm to the public.

(d) Hearing. No license issued under this Part shall be revoked or suspended except after a hearing thereon. The superintendent shall give a Licensee no less than ten days' written notice of the time and place of such hearing by registered or certified mail addressed to the principal place of business of such Licensee. Any order of the superintendent suspending or revoking such license shall state the grounds upon which it is based and be sent by registered or certified mail to the Licensee at its principal place of business as shown in the records of the Department.

(e) Preliminary injunction. The superintendent may, when deemed by the superintendent to be in the public interest, seek a preliminary injunction to restrain a Licensee from continuing to perform acts that violate any provision of this Part, the Financial Services Law, Banking Law, or Insurance Law.

(f) Preservation of powers. Nothing in this Part shall be construed as limiting any power granted to the superintendent under any other provision of the Banking Law, Insurance Law, or Financial Services Law, including any power to investigate possible violations of law, rule, or regulation or to impose penalties or take any other action against any Person for violation of such laws, rules, or regulations.

Statutory Authority: Financial Services Law, sections 102, 301, 302, 305, and 309

Section 200.7 Compliance

(a) Generally. Each Licensee is required to comply with all applicable federal and state laws, rules, and regulations.

(b) Compliance officer. Each Licensee shall designate a qualified individual or individuals responsible for coordinating and monitoring compliance with this Part and all other applicable federal and state laws, rules, and regulations.

(c) Compliance policy. Each Licensee shall maintain and enforce written compliance policies, including policies with respect to anti-fraud, anti–money laundering, cyber security, privacy and

information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body.

Statutory Authority: Financial Services Law, sections 102, 301, and 302

Section 200.8 Capital Requirements

(a) Each Licensee shall maintain at all times such capital as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations. In determining the minimum amount of capital that must be maintained by a Licensee, the superintendent will consider a variety of factors, including but not limited to:

(1) the composition of the Licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset;

(2) the composition of the Licensee's total liabilities, including the size and repayment timing of each type of liability;

(3) the actual and expected volume of the Licensee's Virtual Currency Business Activity;

(4) whether the Licensee is already licensed or regulated by the superintendent under the Financial Services Law, Banking Law, or Insurance Law, or otherwise subject to such laws as a provider of a financial product or service, and whether the Licensee is in good standing in such capacity;

(5) the amount of leverage employed by the Licensee;

(6) the liquidity position of the Licensee; and

(7) the financial protection that the Licensee provides for its customers through its trust account or bond.

(b) Each Licensee shall be permitted to invest its retained earnings and profits in only the following high-quality, investment-grade permissible investments with maturities of up to one year and denominated in United States dollars:

(1) certificates of deposit issued by financial institutions that are regulated by a United States federal or state regulatory agency;

(2) money market funds;

(3) state or municipal bonds;
(4) United States government securities; or
(5) United States government agency securities.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.9 Custody and Protection of Customer Assets

(a) Each Licensee shall maintain a bond or trust account in United States dollars for the benefit of its customers in such form and amount as is acceptable to the superintendent for the protection of the Licensee's customers.
(b) To the extent a Licensee secures, stores, holds, or maintains custody or control of Virtual Currency on behalf of another Person, such Licensee shall hold Virtual Currency of the same type and amount as that which is owed or obligated to such other Person.
(c) Each Licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering assets, including Virtual Currency, held, stored, or maintained by, or under the custody or control of, such Licensee on behalf of another Person.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.10 Material Change to Business

(a) Each Licensee must obtain the superintendent's prior written approval for any plan or proposal to introduce or offer a new product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York Residents.
(b) A "material change" may occur where:
(1) a change is proposed to an existing product, service, or activity that may cause such product, service, or activity to be

materially different from that previously listed on the application for licensing by the superintendent;

(2) the proposed change may raise a legal or regulatory issue about the permissibility of the product, service, or activity; or

(3) the proposed change may raise safety and soundness or operational concerns.

(c) The Licensee shall submit a written plan describing the proposed material change, including a detailed description of the business operations, compliance policies, and the impact on the overall business of the Licensee, as well as such other information as requested by the superintendent.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.11 Change of Control; Mergers and Acquisitions

(a) Change of Control. No action shall be taken, except with the prior written approval of the superintendent, that may result in a change of control of a Licensee.

(1) Prior to any change of control, the Person seeking to acquire control of a Licensee shall submit a written application to the superintendent in a form and substance acceptable to the superintendent, including detailed information about the applicant and all directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries of the applicant, as applicable.

(2) For purposes of this Section, the term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Licensee whether through the ownership of stock of such Licensee or the stock of any Person that possesses such power. Control shall be presumed to exist if a Person, directly or indirectly, owns, controls, or holds with power to vote ten percent or more of the voting stock of a Licensee or of any Person that owns, controls, or holds with power to vote ten percent or more of the voting stock of such Licensee.

(3) The superintendent shall approve or deny every application for a change of control of a Licensee hereunder within 120 days from the filing of an application deemed by the superintendent to be complete. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(4) In determining whether to approve a proposed change of control, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

(b) Mergers and Acquisitions. No action shall be taken, except with the prior written approval of the superintendent, that may result in a merger or acquisition of all or a substantial part of the assets of a Licensee.

(1) Prior to any such merger or acquisition, an application containing a written plan of merger or acquisition shall be submitted to the superintendent by the entities that are to merge or by the acquiring entity, as applicable. Such plan shall be in form and substance satisfactory to the superintendent, and shall specify each entity to be merged, the entity that is to receive into itself the merging entity, or the entity acquiring all or substantially all of the assets of the Licensee, as applicable, and shall describe the terms and conditions of the merger or acquisition and the mode of carrying it into effect.

(2) The superintendent shall approve or deny a proposed merger or a proposed acquisition of all or a substantial part of the assets of a Licensee within 120 days after the submission of the proposed plan to the Department. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(3) In determining whether to so approve a proposed merger or acquisition, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.12 Books and Records

(a) Each Licensee shall, in connection with its Virtual Currency Business Activity, make, keep, and preserve all of its books and records in their original form or native file format for a period of at least ten years from the date of their creation and in a condition that will allow the superintendent to determine whether the Licensee is complying with all applicable laws, rules, and regulations. The books and records maintained by each Licensee shall, without limitation, include:

- **(1)** for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of the parties to the transaction;
- **(2)** a general ledger containing all assets, liabilities, capital, income, expense accounts, and profit and loss accounts;
- **(3)** bank statements and bank reconciliation records;
- **(4)** any statements or valuations sent or provided to customers and counterparties;
- **(5)** records or minutes of meetings of the board of directors or an equivalent governing body;
- **(6)** records demonstrating compliance with applicable state and federal anti–money laundering laws, rules, and regulations, including customer identification and verification documents, records linking customers to their respective accounts and balances, and a record of all compliance breaches;
- **(7)** communications and documentation related to investigations of customer complaints and transaction error resolution or concerning facts giving rise to possible violations of laws, rules, or regulations;
- **(8)** all other records required to be maintained in accordance with this Part; and
- **(9)** all other records as the superintendent may require.

(b) Each Licensee shall provide the Department, upon request, immediate access to all facilities, books, records, documents, or other information maintained by the Licensee or its Affiliates, wherever located.

(c) Records of non-completed, outstanding, or inactive Virtual Currency accounts or transactions shall be maintained for at least five years after the time when any such Virtual Currency has been deemed, under the Abandoned Property Law, to be abandoned property.

Statutory Authority: Financial Services Law, sections 102, 202, 301, 302, and 306

Section 200.13 Examinations

(a) Each Licensee shall permit and assist the superintendent to examine the Licensee whenever in the superintendent's judgment such examination is necessary or advisable, but not less than once every two calendar years, including, without limitation, to determine:
- **(1)** the financial condition of the Licensee;
- **(2)** the safety and soundness of the conduct of its business;
- **(3)** the policies of its management;
- **(4)** whether the requirements of laws, rules, and regulations have been complied with in the administration of its affairs; and
- **(5)** such other matters as the superintendent may determine, including, but not limited to, any activities of the Licensee outside the State of New York if in the opinion of the superintendent such activities may affect the Licensee's business involving New York or New York Residents.

(b) Each Licensee shall permit and assist the superintendent at any time to examine all of the Licensee's books, records, accounts, documents, and other information.

(c) Each Licensee shall permit and assist the superintendent to make such special investigations as the superintendent shall deem necessary to determine whether a Licensee has violated any provision of the applicable laws, rules, or regulations and to the extent necessary shall permit and assist the superintendent to examine all

relevant facilities, books, records, accounts, documents, and other information.

(d) For the purpose of determining the financial condition of the Licensee or its safety and soundness practices, the Licensee shall permit and assist the superintendent, when in the superintendent's judgment it is necessary or advisable, to examine an Affiliate of the Licensee.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.14 Reports and Financial Disclosures

(a) Each Licensee shall submit to the superintendent quarterly financial statements within 45 days following the close of the Licensee's fiscal quarter in the form, and containing such information, as the superintendent shall prescribe, including without limitation, the following information:

- **(1)** a statement of the financial condition of the Licensee, including a complete balance sheet, income statement, profit and loss statement, statement of retained earnings, statement of net liquid assets, statement of net worth, statement of cash flows, and statement of change in ownership equity;
- **(2)** a statement demonstrating compliance with any financial requirements established under this Part;
- **(3)** financial projections and strategic business plans;
- **(4)** a list of all off-balance-sheet items;
- **(5)** a chart of accounts, including a description of each account; and
- **(6)** a report of permissible investments by the Licensee as permitted under this Part.

(b) Each Licensee shall submit audited annual financial statements, prepared in accordance with generally accepted accounting principles, together with an opinion of an independent certified public accountant and an evaluation by such accountant of the accounting procedures and internal controls of the Licensee within one hundred and twenty days of its fiscal year end. All such annual financial statements shall include:

(1) a statement of management's responsibilities for preparing the Licensee's annual financial statements, establishing and maintaining adequate internal controls and procedures for financial reporting, and complying with all applicable laws, rules, and regulations;

(2) an assessment by management of the Licensee's compliance with such applicable laws, rules, and regulations during the fiscal year covered by the financial statements, including management's conclusion as to whether the Licensee has complied with those laws, rules, and regulations during such period; and

(3) certification of the financial statements by an officer or director of the Licensee attesting to the truth and correctness of those statements.

(c) Each Licensee shall notify the superintendent in writing of any criminal action or insolvency proceeding against the Licensee or any of its directors, Principal Stockholders, Principal Officers, and Principal Beneficiaries, as applicable, immediately after the commencement of any such action or proceeding.

(d) Each Licensee shall notify the superintendent in writing of any proposed change to the methodology used to calculate the value of Virtual Currency in Fiat Currency that was submitted to the Department in accordance with Section 200.4 or this Subsection.

(e) Each Licensee shall submit a report to the superintendent immediately upon the discovery of any violation or breach of law, rule, or regulation related to the conduct of activity licensed under this Part.

(f) Each Licensee shall make additional special reports to the superintendent, at such times and in such form, as the superintendent shall prescribe.

Statutory Authority: Financial Services Law, sections 102, 202, 301, 302, and 306

Section 200.15 Anti–money Laundering Program

All values in United States dollars referenced herein must be calculated using the methodology to determine the value of Virtual Currency in Fiat Currency that was approved by the Department under this Part.

(a) Each Licensee shall conduct an initial risk assessment that will consider legal, compliance, financial, and reputational risks associated with the Licensee's activities, services, customers, counterparties, and geographic location and shall establish, maintain, and enforce an anti-money laundering program based thereon. The Licensee shall conduct additional assessments on an annual basis, or more frequently as risks change, and shall modify its anti-money laundering program as appropriate to reflect any such changes.

(b) The anti–money laundering program shall, at a minimum:

(1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable anti-money laundering laws, rules, and regulations;

(2) provide for independent testing for compliance with, and the effectiveness of, the anti–money laundering program to be conducted by qualified personnel of the Licensee or by a qualified outside party, at least annually, the findings of which shall be summarized in a written report submitted to the superintendent;

(3) designate a qualified individual or individuals in compliance responsible for coordinating and monitoring day-to-day compliance with the anti–money laundering program; and

(4) provide ongoing training for appropriate personnel to ensure they have a fulsome understanding of anti–money laundering requirements and to enable them to identify transactions required to be reported and maintain records required to be kept in accordance with this Part.

(c) The anti-money laundering program shall include a written anti–money laundering policy reviewed and approved by the Licensee's board of directors or equivalent governing body.

(d) Each Licensee, as part of its anti–money laundering program, shall maintain records and make reports in the manner set forth below.

(1) Records of Virtual Currency transactions. Each Licensee shall maintain the following information for all transactions involving the payment, receipt, exchange or conversion, purchase, sale, transfer, or transmission of Virtual Currency: the identity and physical addresses of the parties involved, the amount or

value of the transaction, including in what denomination purchased, sold, or transferred, the method of payment, the date(s) on which the transaction was initiated and completed, and a description of the transaction.

(2) Reports on transactions. When a Licensee is involved in a transaction or series of transactions for the receipt, exchange, conversion, purchase, sale, transfer, or transmission of Virtual Currency, in an aggregate amount exceeding the United States dollar value of $10,000 in one day, by one Person, the Licensee shall notify the Department, in a manner prescribed by the superintendent, within 24 hours.

(3) Reporting of Suspicious Activity. Each Licensee shall monitor for transactions that might signify money laundering, tax evasion, or other illegal or criminal activity and notify the Department, in a manner prescribed by the superintendent, immediately upon detection of such a transaction(s).

(i) Each Licensee shall file Suspicious Activity Reports ("SARs") in accordance with applicable federal laws, rules, and regulations.

(ii) Each Licensee that is not required to file SARs under federal law shall file with the superintendent, in a form prescribed by the superintendent, reports of transactions that indicate a possible violation of law or regulation within 30 days from the detection of the facts that constitute a need for filing. Continuing suspicious activity shall be reviewed on an ongoing basis and a suspicious activity report shall be filed within 120 days of the last filing describing continuing activity.

(e) No Licensee shall structure transactions, or assist in the structuring of transactions, to evade reporting requirements under this Part.

(f) No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate the identity of an individual customer or counterparty. Nothing in this Section, however, shall be construed to require a Licensee to make available to the general public the fact or nature of the movement of Virtual Currency by individual customers or counterparties.

(g) Each Licensee shall also maintain, as part of its anti–money laundering program, a customer identification program.

(1) Identification and verification of account holders. When opening an account for a customer, each Licensee must, at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information, and check customers against the Specially Designated Nationals ("SDNs") list maintained by the Office of Foreign Asset Control ("OFAC"), a part of the U.S. Treasury Department. Enhanced due diligence may be required based on additional factors, such as for high risk customers, high-volume accounts, or accounts on which a suspicious activity report has been filed.

(2) Enhanced due diligence for accounts involving foreign entities. Licensees that maintain accounts for non-U.S. Persons and non-U.S. Licensees must establish enhanced due diligence policies, procedures, and controls to detect money laundering, including assessing the risk presented by such accounts based on the nature of the foreign business, the type and purpose of the activity, and the anti-money laundering and supervisory regime of the foreign jurisdiction.

(3) Prohibition on accounts with foreign shell entities. Licensees are prohibited from maintaining relationships of any type in connection with their Virtual Currency Business Activity with entities that do not have a physical presence in any country.

(4) Identification required for large transactions. Each Licensee must require verification of accountholders initiating transactions having a value greater than $3,000.

(h) Each Licensee shall demonstrate that it has risk-based policies, procedures, and practices to ensure, to the maximum extent practicable, compliance with applicable regulations issued by OFAC.

(i) Each Licensee shall have in place appropriate policies and procedures to block or reject specific or impermissible transactions that violate federal or state laws, rules, or regulations.

(j) The individual(s) designated by the Licensee, pursuant to Subsection 200.15(b)(3), shall be responsible for day-to-day operations of the anti–money laundering program and shall, at a minimum:

(1) Monitor changes in anti–money laundering laws, including updated OFAC and SDN lists, and update the program accordingly;

(2) Maintain all records required to be maintained under this Section;

(3) Review all filings required under this Section before submission;

(4) Escalate matters to the board of directors, senior management, or appropriate governing body and seek outside counsel, as appropriate;

(5) Provide periodic reporting, at least annually, to the board of directors, senior management, or appropriate governing body; and

(6) Ensure compliance with relevant training requirements.

Statutory Authority: Financial Services Law, sections 201, 202, 302, and 404

Section 200.16 Cyber Security Program

(a) Generally. Each Licensee shall establish and maintain an effective cyber security program to ensure the availability and functionality of the Licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program shall be designed to perform the following five core cyber security functions:

(1) identify internal and external cyber risks by, at a minimum, identifying the information stored on the Licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;

(2) protect the Licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

(3) detect systems intrusions, data breaches, unauthorized access to systems or information, malware, and other Cyber Security Events;

(4) respond to detected Cyber Security Events to mitigate any negative effects; and

(5) recover from Cyber Security Events and restore normal operations and services.

(b) Policy. Each Licensee shall implement a written cyber security policy setting forth the Licensee's policies and procedures for the protection of its electronic systems and customer and counterparty data stored on those systems, which shall be reviewed and approved by the Licensee's board of directors or equivalent governing body at least annually. The cyber security policy must address the following areas:

(1) information security;

(2) data governance and classification;

(3) access controls;

(4) business continuity and disaster recovery planning and resources;

(5) capacity and performance planning;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and application development and quality assurance;

(9) physical security and environmental controls;

(10) customer data privacy;

(11) vendor and third-party service provider management;

(12) monitoring and implementing changes to core protocols not directly controlled by the Licensee, as applicable; and

(13) incident response.

(c) Chief Information Security Officer. Each Licensee shall designate a qualified employee to serve as the Licensee's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Licensee's cyber security program and enforcing its cyber security policy.

(d) Reporting. Each Licensee shall submit to the Department a report, prepared by the CISO and presented to the Licensee's board of directors or equivalent governing body, at least annually, assessing the availability, functionality, and integrity of the Licensee's

electronic systems, identifying relevant cyber risks to the Licensee, assessing the Licensee's cyber security program, and proposing steps for the redress of any inadequacies identified therein.

(e) Audit. Each Licensee's cyber security program shall, at a minimum, include audit functions as set forth below.

(1) Penetration testing. Each Licensee shall conduct penetration testing of its electronic systems, at least annually, and vulnerability assessment of those systems, at least quarterly.

(2) Audit trail. Each Licensee shall maintain audit trail systems that:

(i) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

(ii) protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;

(iii) protect the integrity of hardware from alteration or tampering, including by limiting access permissions to hardware, enclosing hardware in locked cages, and maintaining logs of physical access to hardware that allows for event reconstruction;

(iv) log system events including, at minimum, access and alterations made to the audit trail systems by the systems or by an authorized user, and all system administrator functions performed on the systems; and

(v) maintain records produced as part of the audit trail for a period of ten years in accordance with the recordkeeping requirements set forth in this Part.

(3) Source code reviews. Each Licensee shall have an independent, qualified third party conduct a source code review of any internally developed proprietary software used in the Licensee's business operations, at least annually.

(f) Personnel and Intelligence. Each Licensee shall:

(1) employ cyber security personnel adequate to manage the Licensee's cyber security risks and to perform the core cyber security functions specified in Subsection 200.16(a)(1)–(5);

(2) provide and require cyber security personnel to attend regular cyber security update and training sessions; and

(3) require key cyber security personnel to take steps to stay abreast of changing cyber security threats and countermeasures.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.17 Business Continuity and Disaster Recovery

(a) Each Licensee shall establish and maintain a written business continuity and disaster recovery ("BCDR") plan reasonably designed to ensure the availability and functionality of the Licensee's services in the event of an emergency or other disruption to the Licensee's normal business activities. The BCDR plan, at minimum, shall:

(1) identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the Licensee's business;

(2) identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;

(3) include a plan to communicate with essential Persons in the event of an emergency or other disruption to the operations of the Licensee, including employees, counterparties, regulatory authorities, data and communication providers, disaster recovery specialists, and any other Persons essential to the recovery of documentation and data and the resumption of operations;

(4) include procedures for the maintenance of back-up facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;

(5) include procedures for the back-up or copying, with sufficient frequency, of documents and data essential to the operations of the Licensee and storing of the information off site; and

(6) identify third parties that are necessary to the continued operations of the Licensee's business.

(b) Each Licensee shall distribute a copy of the BCDR plan, and any revisions thereto, to all relevant employees and shall maintain copies of the BCDR plan at one or more accessible off-site locations.

(c) Each Licensee shall provide relevant training to all employees responsible for implementing the BCDR plan regarding their roles and responsibilities.

(d) Each Licensee shall promptly notify the superintendent of any emergency or other disruption to its operations that may affect its ability to fulfill regulatory obligations or that may have a significant adverse effect on the Licensee, its counterparties, or the market.

(e) The BCDR plan shall be tested at least annually by qualified, independent internal personnel or a qualified third party, and revised accordingly.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.18 Advertising and Marketing

(a) Each Licensee engaged in Virtual Currency Business Activity shall not advertise its products, services, or activities in New York or to New York Residents without including the name of the Licensee and the legend that such Licensee is "Licensed to engage in Virtual Currency Business Activity by the New York State Department of Financial Services."

(b) Each Licensee shall maintain, for examination by the superintendent, all advertising and marketing materials, including but not limited to print media, internet media (including websites), radio and television advertising, road show materials, presentations, and brochures. Each Licensee shall maintain hard copy, website captures, and audio and video scripts of its advertising and marketing materials, as applicable.

(c) In all advertising and marketing materials, each Licensee shall comply with all disclosure requirements under federal and state laws, rules, and regulations.

(d) In all advertising and marketing materials, each Licensee and any person or entity acting on its behalf, shall not, directly or by implication, make any false, misleading, or deceptive representations or omissions.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.19 Consumer Protection

(a) Disclosure of material risks. As part of establishing a relationship with a customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all material risks associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following:

(1) virtual currency is not legal tender, is not backed by the government, and accounts and value balances are not subject to Federal Deposit Insurance Corporation or Securities Investor Protection Corporation protections;

(2) legislative and regulatory changes or actions at the state, federal, or international level may adversely affect the use, transfer, exchange, and value of Virtual Currency;

(3) transactions in Virtual Currency are generally irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

(4) some Virtual Currency transactions shall be deemed to be made when recorded on a "block chain" ledger, which is not necessarily the date or time that the customer initiates the transaction;

(5) the value of Virtual Currency is derived from the continued willingness of market participants to exchange Fiat Currency for Virtual Currency, which may result in the potential for permanent and total loss of value of a particular Virtual Currency should the market for that Virtual Currency disappear;

(6) there is no assurance that a Person who accepts a Virtual Currency as payment today will continue to do so in the future;

(7) the volatility and unpredictability of the price of Virtual Currency relative to Fiat Currency may result in significant loss or tax liability over a short period of time;

(8) the nature of Virtual Currency may lead to an increased risk of fraud or cyber attack;

(9) the nature of Virtual Currency means that any technological difficulties experienced by the Licensee may prevent the access or use of a customer's Virtual Currency; and

(10) any bond or trust account for the benefit of customers may not be sufficient to cover any and all losses incurred by customers.

(b) Disclosure of general terms and conditions. When opening an account for a new customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all relevant terms and conditions associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following, as applicable:

(1) the customer's liability for unauthorized Virtual Currency transactions;

(2) the customer's right to stop payment of a preauthorized Virtual Currency transfer and the procedure to initiate such a stop-payment order;

(3) the Licensee's liability to the customer under any applicable federal or state laws, rules, or regulations;

(4) under what circumstances the Licensee will, absent a court or government order, disclose information concerning the customer's account to third parties;

(5) the customer's right to receive periodic account statements and valuations from the Licensee;

(6) the customer's right to receive a receipt, trade ticket, or other evidence of a transaction;

(7) the customer's right to prior notice of a change in the Licensee's rules or policies; and

(8) such other disclosures as are customarily given in connection with the opening of customer accounts.

(c) Disclosures of the terms of transactions. Prior to each transaction in Virtual Currency, for, on behalf of, or with a customer, each Licensee shall furnish to each such customer a written disclosure in clear, conspicuous, and legible writing in the English language and

in any other predominant language spoken by the customers of the Licensee, containing the terms and conditions of the transaction, which shall include, at a minimum, to the extent applicable:

(1) the amount of the transaction;

(2) any fees, expenses, and charges borne by the customer, including applicable exchange rates;

(3) the type and nature of the Virtual Currency transaction;

(4) a warning that once executed the transaction may not be undone, if applicable; and

(5) such other disclosures as are customarily given in connection with a transaction of this nature.

(d) Acknowledgement of disclosures. Each Licensee shall ensure that all disclosures required in this Section are acknowledged as received by customers.

(e) Receipts. Upon completion of any transaction, each Licensee shall provide to a customer a receipt containing the following information:

(1) the name and contact information of the Licensee, including a telephone number established by the Licensee to answer questions and register complaints;

(2) the type, value, date, and precise time of the transaction;

(3) the fee charged;

(4) the exchange rate, if applicable;

(5) a statement of the liability of the Licensee for non-delivery or delayed delivery;

(6) a statement of the refund policy of the Licensee; and

(7) any additional information the superintendent may require.

(f) Each Licensee shall make available to the Department, upon request, the form of the receipts it is required to provide to customers in accordance with Subsection 200.19(e).

(g) Prevention of fraud. Licensees are prohibited from engaging in fraudulent activity and customers of Licensees that are victims of fraud shall be entitled to claim compensation from any trust account, bond, or insurance policy maintained by the Licensee. Additionally, each Licensee shall take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy shall, at a minimum, include:

(1) the identification and assessment of fraud-related risk areas;
(2) procedures and controls to protect against identified risks;
(3) allocation of responsibility for monitoring risks; and
(4) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

Statutory Authority: Financial Services Law, sections 102, 201, 202, 301, 302, 306, and 404

Section 200.20 Complaints

(a) Each Licensee shall establish and maintain written policies and procedures to fairly and timely resolve complaints.
(b) Each Licensee must provide, in a clear and conspicuous manner, on its website(s), in any physical location(s), and in any other location as the superintendent may prescribe, the following disclosures:
  (1) the Licensee's mailing address, email address, and telephone number for the receipt of complaints;
  (2) a statement that the complainant may also bring his or her complaint to the attention of the Department;
  (3) the Department's mailing address, website, and telephone number; and
  (4) such other information as the superintendent may require.
(c) Each Licensee shall report to the superintendent any change in the Licensee's complaint policies or procedures within seven days.

Statutory Authority: Financial Services Law, sections 102, 201, 202, 301, and 302

Section 200.21 Transitional Period

A Person already engaged in Virtual Currency Business Activity must apply for a license in accordance with this Part within 45 days of the effective date of this regulation. In doing so, such applicant shall be deemed in compliance with the licensure requirements of this Part until it has been notified by the superintendent that its application has been denied, in which case it shall immediately cease operation in this state.

Any Person engaged in Virtual Currency Business Activity that fails to submit an application for a license within 45 days of the effective date of this regulation shall be deemed to be conducting unlicensed Virtual Currency Business Activity.

Statutory Authority: Financial Services Law, sections 202, 206, 302, 303, 305, 306, 309, 404, and 408; Executive Law, section 63

Index

Note: Page references in *italics* refer to figures.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.