THE BITCOIN
BIG BANG
For my wife, Dawn, this book is a testament to your unwavering faith in my stupid ideas.
Contents

Preface xi
Acknowledgments xiii
About the Author xv

Chapter 1  Bitcoin Is a Bubble 1
The Quest to Buy Bitcoin 3
Bitcoin Enlightenment 6
Currencies Are a Matter of Trust 8
What Is Bitcoin? 10
Is It a Currency? 13
It’s Revolutionary 17

Chapter 2  Understanding the Digital Gold Rush 19
The Language of Bitcoin 22
How Do I Buy Bitcoin? 26
Who “Gets” It? 30
The Gold Rush Is Just Starting 31

Chapter 3  Bitcoin Is More than Digital Gold 33
Searching for Satoshi 34
The Search 37
Why Is Satoshi a Genius? 44
Bigger than Satoshi 46

Chapter 4 Byzantine Generals’ Problem 49
How Does Bitcoin Solve the BGP? 52
51 Percent Attack 55
An Elegant Solution 57

Chapter 5 A Decentralized Financial System 59
Grand De-Central Station 63
What’s at Stake? 69
Central Banks 72
Bitcoin Is the Catalyst 73

Chapter 6 What Do You Call a Bitcoin Miner? 75
A Banker 77
How Does a Bitcoin Transaction Work? 77
What Is Cryptography? 78
Still Want to Be a Miner? 82
Do We Need Another Bitcoin? 88

Chapter 7 Nautiluscoin—0 to $1 Million in 60 Days 91
Creating the Coin 94
Did It Work? 104

Chapter 8 Building the Nautiluscoin Economy 107
Dynamic Proof-of-Stake 110
Other Policy Tools 113
Alternative to Gold 115
Money, Made Better 116
Financial Market Integration 117
Special Drawing Rights 119
Why NAUT? 119

Chapter 9 Investing and Trading in Alternative Currencies 121
A New Investment Class 123
Valuation 129
Exchanges 133
Investment Vehicles 134
Asset Class Growth 136
Chapter 10  Regulation  139
  Regulatory Agencies  140
  Challenges to Regulation  147
  Pushing on a String  147

Chapter 11  Smart Money: Set It and Forget It  149
  Rules of the Road  151
  Smart Contracts and Property  152
  Ethereum  155
  Cryptoequities: A New Type of Investment  160
  Decentralized Autonomous Organizations  161
  Professor Money  162

Chapter 12  Everything You Know about Business Is Wrong  163
  Cryptonomics  166
  Growth Share Matrix  169
  Learning Curve Effects  171
  Porter’s Three Generic Strategies  172
  Human Resource Management  173
  Fueling the Sharing Economy  174
  The Future Just Might Work  176

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  179
  Currency vs. Virtual Currency  180
  Background  180
  Definitions of User, Exchanger, and Administrator  181
  Users of Virtual Currency  181
  Administrators and Exchangers of Virtual Currency  182
  Providers and Sellers of Prepaid Access  185
  Dealers in Foreign Exchange  186
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
Section 200.2 Definitions
Section 200.3 License
Section 200.4 Application
Section 200.5 Application Fees
Section 200.6 Action by Superintendent
Section 200.7 Compliance
Section 200.8 Capital Requirements
Section 200.9 Custody and Protection of Customer Assets
Section 200.10 Material Change to Business
Section 200.11 Change of Control; Mergers and Acquisitions
Section 200.12 Books and Records
Section 200.13 Examinations
Section 200.14 Reports and Financial Disclosures
Section 200.15 Anti–Money Laundering Program
Section 200.16 Cyber Security Program
Section 200.17 Business Continuity and Disaster Recovery
Section 200.18 Advertising and Marketing
Section 200.19 Consumer Protection
Section 200.20 Complaints
Section 200.21 Transitional Period

Index
very 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
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 communica-
tion. The collision of personal computers and the Internet spawned com-
panies 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 with-
out 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