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.