The Ultimate Guide to bitcoin™

Michael Miller

The Ultimate Guide to Bitcoin™

MICHAEL MILLER

que®

800 East 96th Street,
Indianapolis, Indiana 46240 USA

The Ultimate Guide to Bitcoin™

ISBN-13: 978-0-7897-5324-3
ISBN-10: 0-7897-5324-3

Library of Congress Control Number: 2014942081

Printed in the United States of America

First Printing: October 2014

Trademarks

Warning and Disclaimer

Special Sales

Editor-in-Chief
Greg Wiegand

Executive Editor
Rick Kughen

Managing Editor
Kristy Hart

Project Editors
Melissa Schirmer
Elaine Wiley

Copy Editor
Cheri Clark

Senior Indexer
Cheryl Lenser

Proofreader
Katie Matejka

Technical Editor
Timothy L. Warner

Publishing Coordinator
Kristin Watterson

Cover Designer
Mark Shirar

Senior Compositor
Gloria Schurick

CONTENTS AT A GLANCE

TABLE OF CONTENTS

About the Author

Michael Miller has written more than 150 non-fiction how-to books over the past two decades, as well as a variety of web articles. His best-selling books include Que's *Absolute Beginner's Guide to Computer Basics*, *The Ultimate Digital Music Guide*, and *Is It Safe? Protecting Your Computer, Your Business, and Yourself Online*. Collectively, his books have sold more than 1 million copies worldwide.

Miller has established a reputation for clearly explaining technical topics to non-technical readers, and for offering useful real-world advice about complicated topics. More information can be found at the author's website, located at www.molehillgroup.com.

Dedication

To grandkids Collin, Alethia, Hayley, Judah, and Lael, and whatever currency you'll be using when you grow up.

Acknowledgments

Thanks to the usual suspects at Que, including but not limited to Rick Kughen, Melissa Schirmer, Elaine Wiley, Cheri Clark, and technical editor Timothy Warner.

We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@quepublishing.com

Mail: Que Publishing
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at quepublishing.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

Bitcoin is like nothing you've ever dealt with before. It's a form of money, but it doesn't physically exist as a coin or paper currency. You can spend it (at some merchants) or save it, or even buy and trade it as a type of speculative commodity. Some people have gotten rich trading in Bitcoin; others have been burned by fraud and hacks and just plain incompetence. And everybody's talking about it, even though few really understand what it's all about.

Some people think that Bitcoin is the currency of the future, destined to replace dollars and euros and other traditional currency. Other people think Bitcoin is a get-rich-quick scheme, this week's bubble that's bound to burst. Others think Bitcoin is a complete and total scam.

The reality is that Bitcoin is potentially all of these things, and none of them. It's what we call a cryptocurrency (because it's based on cryptography technology) or virtual currency (because it doesn't exist in physical form). It's still in its infancy, used by few but monitored by many. And it might be a big part of your personal financial future.

What is Bitcoin good for? Who uses it? How do you get some—and how do you spend any you've gotten? What's it worth? And just how safe is it, anyway?

These are all rational questions for which there are rational answers. Which is why I wrote this book.

The Ultimate Guide to Bitcoin is meant to be…well, the ultimate guide to Bitcoin. It explains what Bitcoin is, why it exists, how it works, who uses it, and more. On the surface, anyway, Bitcoin is easier to understand than you might think. Yes, there's a lot of detail under the surface (and we cover that too), but I try to present the basics of Bitcoin in a way that even the most inexperienced novice will understand. It's not rocket science—just some beginning-level finance and technology.

I assume that you're reading this book to learn about Bitcoin, perhaps with the expectation to start trading, accumulating, or spending Bitcoin. Before you invest your first dollar into this new virtual currency, you want to know what you're getting into. Fair enough; I'll tell you what you need to know to get started.

By the way, I am neither a Bitcoin cheerleader nor a naysayer. You can find plenty of both on the Internet, so you don't need any more biased opinions here. Instead, I try to present the facts as we know them, balanced by realistic descriptions of the risks and rewards of working with Bitcoin. I don't have a horse in this race, but just want to help you make better decisions. I hope you'll find my words useful.

What You Need to Know to Use This Book

How much prior experience with Bitcoin do you need before starting this book? None. In fact, I expect that you have never traded a Bitcoin in your life, and know little about Bitcoin and other cryptocurrencies. That's why you're reading this book, after all. In the world of Bitcoin, we're all novices.

In other words, you don't have to be an experienced Bitcoin trader to dive into this book. The information on these pages is actually best consumed *before* you get involved with Bitcoin—it's the information that beginners need in order to be a little more savvy about the whole Bitcoin thing.

Learn More…

Bitcoin as a topic, a technology, and a currency is in constant flux. It's not just the pricing that's volatile; not a day goes by without some seemingly major development or announcement concerning Bitcoin or other cryptocurrencies.

That means that some of the information in this book will be outdated by the time you read these words. That's simply to be expected—and especially true in regard to any discussion of Bitcoin pricing. If I write something about a $500 price and, when you read the book, the current price is $700 (or $300), accept that things have changed and make the necessary conversions. There's really no way of predicting these things, so we just have to deal with them.

As to keeping abreast of Bitcoin-related developments, a handful of websites report daily Bitcoin-related news and deliver the latest exchange rates and other statistics. If you're serious about Bitcoin, bookmark these sites and make them a component of your daily reading regimen:

- Bitcoin Magazine (www.bitcoinmagazine.com)
- Blockchain (www.blockchain.info)
- CoinDesk (www.coindesk.com)
- CoinReport (www.coinreport.net)
- CryptoCoinsNews (www.cryptocoinsnews.com)

In addition, I recommend you subscribe to the Bitcoin News' Twitter feed, @bitcoinnews, and to the r/Bitcoin subreddit on Reddit (www.reddit.com/r/Bitcoin/). Both are good sources of up-to-the-minute news, rumors, and discussions.

Finally, there are two Bitcoin-related discussion forums worth your participation. Both of these Bitcoin forums, www.bitcointalk.org and www.bitcoinforum.org, are filled with real and imagined experts on everything Bitcoin, and they will help you get involved with the greater Bitcoin community. Take a look and join in as you like.

3

A Short History of Bitcoin

So Bitcoin is a virtual currency. But how did Bitcoin come about? How did Bitcoin evolve from concept to the most popular virtual currency today?

Virtual Currency Before Bitcoin

Although Bitcoin is the best-known virtual currency, it wasn't the first. In fact, Bitcoin is just the latest of a multitude of schemes designed to supplement or replace traditional money.

E-gold

One of the first virtual currencies was E-gold, founded in 1996. E-gold was unique in that its virtual currency was backed by real, honest-to-goodness gold bullion. In essence, trading E-gold was basically the same as swapping gold ownership, but anonymously.

At its peak, in 2008, E-gold claimed more than five million user accounts. However, the anonymous nature of the currency made the service very attractive to crime syndicates looking to launder their dirty dollars into cleaner cash. Weak security systems also contributed to an influx of hacking and fraud from these same crime syndicates.

E-gold's calling card.

All of this led the U.S. government to get involved, and in 2008 the company's management pleaded guilty to money laundering and operating an unlicensed money transfer business. The Feds froze all user accounts, amounting to more than $86 million in E-gold. The company itself closed its doors the following year.

By the way, E-gold was just one of several similar virtual gold payment systems back in the day. Competitors included GoldMoney and e-Bullion, which appeared equally shady. (E-Bullion's owner was eventually arrested on charges of running an illegal money transfer business and of paying three hit men to stab his wife to death. Good folks there.)

Beenz and Flooz

In 1998, an interesting new website called Beenz.com was launched. The idea behind Beenz.com is that you could earn virtual currency (called Beenz) for performing a variety of online activities, such as visiting certain websites or shopping online. The Beenz you earned could then be spent on various online goods and services.

The site tried to position itself as "the web's currency" that would challenge the world's traditional currencies. That it didn't succeed is now obvious. In fact, Beenz had a very short life, closing its virtual doors in 2001. It never got past the challenge of convincing governments around the world that it really wasn't establishing a new currency, or of convincing users that it wasn't all a big scam.

The Beenz.com website in 2001.

Similar to Beenz was Flooz, which was promoted by none other than comedian Whoopi Goldberg. Flooz was as big a joke as Beenz was, and operated in much the same fashion, trying to establish a unique online currency for use with Internet merchants. Flooz launched in 1999 and closed in 2001, never having attracted much of a user base.

Q Coins

The Chinese Internet service provider Tencent has a very successful instant messaging service called QQ. Back in 2002, QQ developed its own internal virtual currency, called Q Coins, that customers could use to purchase various virtual goods and services, such as extra storage space, virtual pets, and online game avatars.

Over the next few years, various non-QQ online merchants began accepting Q Coins for real-world goods and services. More than 100 million Chinese ended up using Q Coins, generating a trading volume in Q Coins of several billion yuan a year. Eventually, Q Coins ended up being so popular that they were being traded on China's black market for whatever it is that the Chinese trade on the black market. This so concerned the Chinese government that it eventually cracked down on the real-world trading of Q Coins—although they're still used today within the QQ service.

(China's experience with Q Coins no doubt led to their recent crackdown in Bitcoin trading. They've been through all this before.)

Linden Dollars

The concept of virtual currency makes a lot of sense within online virtual worlds. Case in point, the virtual world of Second Life and its very popular virtual currency, Linden Dollars.

For those unfamiliar with virtual worlds, these are online communities that take the form of interactive simulated environments—kind of like a massive multiplayer video game. Users inhabit the world's graphical three-dimensional environment and interact with one another via cartoon-like avatars, often participating in virtual activities and—this is important—economies.

The economy part comes in when users want to buy things within the virtual world, such as virtual clothing for their avatars, virtual housing, virtual entertainment, you name it. For this reason, most virtual worlds have their own unique virtual currencies that can be spent only within the confines of the online world.

Thus it was with Second Life, which was one of the—if not *the*—most popular virtual worlds. Second Life was developed by a company called Linden Lab back in 2003, and its proprietary virtual currency was dubbed Linden Dollar. Users could purchase Linden Dollars (abbreviated L$) using U.S. dollars and other real-world currency on Second Life's LindeX exchange, or from other users or independent brokers.

Buying Linden Dollars in Second Life.

Second Life and its Linden Dollar currency became so popular that tons of real-world companies, including American Apparel, Reebok, and Ford, established presences within Second Life. These companies accepted payment for both virtual and real-world goods and services in Linden Dollars.

The growth in Second Life and its virtual currency eventually led serious investors to speculate in Linden Dollars. In fact, virtual investment banks arose to facilitate Second Life currency trading.

All good things come to an end, however. In 2007, Second Life virtual investment bank Ginko Financial collapsed, leaving users unable to retrieve approximately $750,000 worth of Linden Dollars that had been invested. This led to Linden Labs officially banning all virtual banks in Second Life, as well as removing all objects related to in-world virtual banking.

Over the next several years, interest in Second Life began to wane. Second Life is still around, but it's a shadow of its former self. You can still trade Linden Dollars for U.S. dollars (and other currency), but you'd be hard-pressed to find many buyers.

Facebook Credits

In-world virtual currencies are not the sole province of online games and virtual worlds. Many bit-time social media sites have at least experimented with the concept of their own proprietary virtual currencies.

Take Facebook, for example. In 2009 Facebook began testing the concept of Facebook Credits, which could be used to pay for in-game goods and services on the Facebook site. Facebook Credits went live in January 2011, and users could purchase 10 Facebook Credits for one U.S. dollar.

Purchasing Facebook Credits in 2011.

Much to Facebook's chagrin, Facebook Credits never really took off. Facebook killed the project in June of 2012, converting all remaining Facebook Credits into standard dollar (or other currency) credits to users' accounts.

And More...

As you can see, a plethora of various virtual currency schemes have been floated (and mainly sunk) over the past 15 years or so. In addition to the currencies already mentioned, you run across others such as Dexit, DigiCash, eCache, eCash, InternetCash, Pecunix, and WebMoney. (Google them if you're interested.) What all these virtual currencies have in common is that they are failures. For one reason or another, none of these virtual currencies managed to make it into the mainstream; at best, some existed within their own virtual worlds, but that's the extent of it.

That doesn't mean that all virtual currencies are destined to fail, however. Which brings us to the next stage in our history lesson: the birth of Bitcoin.

GOLD FARMING

The concept of in-world or in-game virtual currencies is an interesting one—especially when you layer in the ability to trade online goods for real-world currency. Here's what happens.

Game players want to buy virtual things in their virtual worlds, but don't want to (or can't) build up the currency via normal in-world means. So they pay other players real-world cash for the in-game currency that the other players

have built up by playing the game. In other words, if you want to level up, you can pay for some other player's tokens that get you to that level.

The problem comes when individuals or groups of individuals start doing this for a profit—that is, selling their in-game credits for real money. This is called *gold farming*, and it's a real thing. (And a big enough deal that many games ban the practice.)

It's also a source of something resembling slave labor. Apparently, work camp inmates in China have been forced to play online games to accumulate online goods and credits that are then sold for real-world currency. It's kind of a virtual sweatshop, when you think about it.

Then Came Bitcoin

Bitcoin has been around for only about a half-dozen years. It has been a short but eventful life, with the Bitcoin economy rising from nothing to close to $6 billion today.

Pre-2008: Crypto-Anarchy

Throughout the 1990s and 2000s, there arose considerable interest, in some circles, in cryptology and crypto-anarchy. If you've never heard of crypto-anarchy, know that it involves the employment of cryptographic tools to avoid detection (and often prosecution) when sending and receiving information over the Internet and other computer networks. Crypto-anarchists tend to be motivated by one (or more) of three main issues. First, defending against the unwanted surveillance of Internet-based communications. Second, defending against Internet censorship. And third, participating in what they call "counter economics," in essence conducting economic transactions outside of traditional financial systems and across national boundaries, often for illicit reasons.

It's this last motive that inspired some of the leading crypto-anarchists to turn their attention toward cryptocurrency. This led to the development of several pre-Bitcoin virtual currency concepts, including Wei Dai's b-money, Nick Szabo's bit gold, and Hal Finney's RPOW. None of these ideas made it much past the conceptual stages, however—although all were obvious influences on what came next.

2008: Gestation

The world (or some part of it) first heard about this thing called Bitcoin in August of 2008. Two things happened then. First, on August 15, Charles Bry, Neal King, and Vladimir Oksman—three scientists/academics working in the field of

encryption—filed a patent application for an invention for updating and distributing encryption keys. Second, on August 18, the domain name bitcoin.org was registered. Something was definitely in the works.

The big bombshell dropped on October 31, 2008, when a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was posted to the Internet. This paper detailed the methods of using peer-to-peer (P2P) networking to facilitate electronic transactions—essentially spelling out all the ideas behind the concept of Bitcoin. (You can read the paper yourself online at bitcoin.org/bitcoin.pdf. It's only 8 pages long and easy enough to digest.)

The author of that paper, and the de facto founder of Bitcoin, went by the name of Satoshi Nakamoto—in retrospect, a fictitious name for a secretive character. But back then Nakamoto was onto something important, and on November 9 he registered the Bitcoin project at SourceForge.net, the home of much open-source software development. There was more to come.

WILL THE REAL SATOSHI NAKAMOTO PLEASE STAND UP?

The original paper that detailed the workings of Bitcoin was written pseudonymously by someone called "Satoshi Nakamoto." This same person was personally responsible for developing the bulk of the Bitcoin software and also posted relevant technical information about the Bitcoin project on the semiofficial BitcoinTalk Forum.

The question is, who is Satoshi Nakamoto? He has never revealed his true identity, although there has been much speculation over the years.

Fast Company magazine, for example, conducted an investigation that strongly suggested that "Satoshi Nakamoto" was actually a collective composed of Charles Bry, Neal King, and Vladimir Oksman—the three scientists who filed for that encryption patent back in 2008. All three individuals denied being Mr. Nakamoto, however, so the search continued.

The New Yorker magazine conducted its own in-depth investigation into Nakamoto's identity and turned up two possible candidates: Irish computer science student Michael Clear and Vili Lehdonvirta, a Research Fellow at the Oxford Internet Institute. But both of these suspects denied being the man in question, so that exploration was for naught.

Other individuals speculated to be the man behind the currency include Japanese mathematician Shinichi Mochizuki, programmer Wei Dai (developer of Bitcoin predecessor b-money), digital currency researcher Nick Szabo (developer of bit-gold, another Bitcoin predecessor), and software developer

and cryptographic activist Hal Finney (developer of yet another pre-Bitcoin virtual currency concept, dubbed RPOW). Despite the "proof" offered for each of the candidates, all have denied being the man behind the currency.

In a March 2014 *Newsweek* article, journalist Leah McGrath Goodman took a simpler approach and started looking for men actually named "Satoshi Nakamoto." She found one in Temple City, California, a reclusive 64-year-old physicist named Dorian S. Nakamoto. (The "S" is for Satoshi, naturally.) This Nakamoto denied being the man in question, however, and hired a lawyer to clear his name. So much for the simple approach.

Whoever he is or was, Satoshi Nakamoto hasn't been involved with the Bitcoin community since mid-2010. His last communication was in April of 2011, when he said he had "moved on to other things."

Thank you, Mr. Nakamoto, and good night.

2009: Birth

The development of Bitcoin continued apace, and on January 3, 2009, Nakamoto mined the very first Bitcoins, the so-called "genesis block." On January 9, he released the first open-source Bitcoin client (v0.1). Three days later, on January 12, the first Bitcoin transaction was recorded, from Nakamoto to Hal Finney—a name you've heard before.

Finney was (and is) a developer at PGP Corporation, a company at the forefront of public-key cryptography—the technology behind Bitcoin's encryption capabilities. He is also a noted activist in the field of cryptography, responsible for running several anonymous remailer servers and staging a contest to break Netscape's export-grade encryption. In 2004, Finney created the first reusable proof-of-work protocol, dubbed RPOW, which was a system that required some work from the service requester before a credit of some sort would be applied; a version of this protocol was incorporated into the Bitcoin mining process. It goes without saying, then, that Finney was integral to the creation of Bitcoin (which is why some claim that Finney himself is actually Satoshi Nakamoto—which Finney, of course, denies).

Back to our story, and to that first Bitcoin transaction. This first transaction created what is known as the *genesis block*, the initial block in the ever-growing Bitcoin block chain. Nakamoto's genesis block was composed of 50 Bitcoins—50 BTC, in Bitcoin parlance. The value of those first Bitcoin transactions was negotiated by individuals on the bitcointalk forums, which is where all interested parties hung out online. (You can access the bitcointalk forums today at https://bitcointalk.org.)

Throughout the balance of 2009, Nakamoto and others continued to work on the Bitcoin technology and the associated trading process. During these early days there were no formal Bitcoin exchanges; all the trading took place between individuals on the bitcointalk forums. For example, in October of 2009, forum member NewLibertyStandard set the exchange rate of 1 dollar equaling 1,309.03 BTC, or $0.0007/BTC. (Bitcoins weren't worth a whole lot back then.)

2010: Getting Real

It wasn't long before the first "official" (or as official as anything can be in the decentralized world of virtual currency) Bitcoin exchange was established. Trading at Bitcoin Market, owned and operated by bitcointalk member dwdollar, began on February 6, 2010. As of May 2010, the exchange rate on Bitcoin Market was $0.004/BTC.

Of course, the exchange rate fluctuated based on supply and demand, and there was little of either. For example, bitcointalk member laslo established the exchange rate of $0.0025/BTC by paying jercos, another user, 10,000 BTC for two pizzas worth approximately $25.

July of 2010 saw the establishment of another Bitcoin exchange named Mt. Gox. (Remember that name; it becomes very important later on.) Mt. Gox actually got its start in 2007 as an online exchange for *Magic: The Gathering Online* trading cards; the name comes from **M**agic **T**he **G**athering **O**nline e**X**change. The site went through several different permutations before settling in as a Bitcoin exchange.

Before Mt. Gox opened, the Bitcoin exchange rate was $0.008/BTC. Five days later the value had increased tenfold, to $0.08/BTC. (This increase in value was also due in part to an influx of new Bitcoin users, as v0.03 of the Bitcoin software was released that month.)

In August of 2010, a major vulnerability in the Bitcoin protocol arose, which enabled users to bypass Bitcoin's built-in restrictions and create an indefinite number of Bitcoins. This was not a good thing, as more than 184 billion BTCs were generated in a single transaction on August 15, effectively making worthless the entire currency. Fortunately, the fraudulent transaction was quickly spotted and reversed, and the bug was fixed—not yet to be repeated.

That little setback out of the way, the Bitcoin exchange rate continued to climb throughout the rest of the year, reaching $0.50/BTC. By November, the total value of the Bitcoin economy surpassed $1 million.

2011: Ups and Downs

By January of 2011, 5.25 million Bitcoins had been generated. On February 9, 2011, Bitcoin reached parity with the U.S. dollar, with Mt. Gox reporting an even exchange rate of $1.00/BTC.

This increase in the exchange rate resulted in an even larger influx of users. The exchange rate subsequently declined, however, dropping to $0.70/BTC by the middle of March.

In April of 2011, *TIME* magazine provided even more exposure by publishing one of the articles about Bitcoin in the mainstream press. Not coincidentally, the value of the Bitcoin economy passed $10 million by the end of that month.

Mt. Gox had quickly become the largest Bitcoin exchange, but several others were launched throughout 2011. These included exchanges for British pound sterling (Britcoin), Brazilian real (Bitcoin Brazil), and Polish zloty (BitMarket.eu).

After the *TIME* story, the Bitcoin exchange rate saw a rapid rise. The rate hit $10.00/BTC in June and peaked at $31.91/BTC on June 8. This gave the Bitcoin economy a $206 million market capitalization. However, that peak was followed by a precipitous drop just four days later, when the exchange rate went back down to $10.00/BTC again. This was a good demonstration of the volatility of the Bitcoin market.

Then the unthinkable happened. On June 15, 2011, the Mt. Gox database was hacked and fake sell orders were placed for more than 25,000 BTC from 478 user accounts. This drove the price of Bitcoins (at Mt. Gox, anyway) down to $0.01/BTC. This would have wiped out hundreds of investors, except that Mt. Gox was able to reverse all the phony trades.

That wasn't the only low point for Bitcoin in 2011. In July, the operator of Bitomat, the third-largest Bitcoin exchange, announced that he had lost access to the wallet.dat file that held approximately 17,000 BTC, worth about $220,000 at the time. The operator announced that he would sell the service for the missing amount, intending to use funds from the sale to refund his customers.

In August another Bitcoin exchange, MyBitcoin, was hacked. This caused the exchange to shut down, refunding just 49% of customer deposits, for a loss of nearly $800,000.

Despite those obvious lows, there were plenty of high points in the world of Bitcoin in 2011. For example, in July of 2011, Intervex Digital released BitCoins Mobile, the first Bitcoin app for iOS devices. In August, the first Bitcoin Conference and World Expo was held in New York City. And in November, the first European Bitcoin Conference was held in Prague.

2012: Rocky Times

Let's face it, 2012 wasn't the best of years for those trading in Bitcoins. Not only did the price of Bitcoins not increase much, ending the year at just $13/BTC, but it also was a time of much internal turmoil and criminal activity.

For example, in March close to 50,000 BTC was stolen from the Linode exchange. And in September the Bitfloor exchange was hacked, with more than 24,000 BTC stolen.

In August, a lawsuit was filed against the Bitcoinica exchange, as a result of close to a half-million dollars in lost savings. The exchange was hacked twice in 2012, which led to allegations that Bitcoinica neglected the safety of its customers' investments.

August also saw the closing of the Bitcoin Savings and Trust, which left around $5.6 million in Bitcoin-based debts. This led to an investigation by the SEC of the exchange as being kind of a Ponzi scheme.

The news in 2012 wasn't all bad, however. In December Bitcoin-Central (now called Paymium) became the first Bitcoin exchange licensed as a bank in Europe, which put a veneer of respectability on the whole endeavor.

2013: Looking Up (Sort Of...)

After the dismal year prior, 2013 looked to be a bit of an improvement for the world of Bitcoin. It started with a very healthy increase in the currency's value, with the exchange rate breaking the 2011 peak of $31.91/BTC on February 28, 2013. The price continued to rise over the next few months, breaking $100/BTC by the first of April. At that point the Bitcoin market cap passed $1 billion.

Later in April, Bitcoin exchanges Mt. Gox and BitInstant had problems due to insufficient capacity, which resulted in delays in processing trades. This caused the exchange rate, which had risen to $266/BTC, to quickly drop to $55/BTC. (The rate stabilized near $160/BTC within a few hours of the issue, however.)

Mt. Gox saw more problems in May, when the U.S. Department of Homeland Security seized more than $5 million from its U.S. accounts. The reason was that Mt. Gox had not registered as a Money Service Business (MSB) with the government's Financial Crimes Enforcement Network (FinCEN). FinCEN had earlier established new regulatory guidelines for what it called "decentralized virtual currencies" that classified Bitcoin miners and exchanges as MSBs—and, as such, subject to registration and other legal requirements. (For example, FinCEN's guidelines require Bitcoin exchanges to disclose large transactions and suspicious activity, comply with money-laundering regulations, and collect information about

their customers.) Because Mt. Gox hadn't yet registered, the government took action.

The exchange got a reprieve in June, when it finally received its MSB license from FinCEN. Mt. Gox's problems didn't end there, however. The exchange suspended withdrawals in U.S. dollars on June 20, after which the Tokyo branch of the Mizuho Bank (which handled all of Mt. Gox's transactions) pressured the exchange to close its account. Mt. Gox announced that it fully resumed withdrawals on July 4, although users reported that few withdrawals in U.S. dollars had been successfully completed. By November, it was reported that Mt. Gox users around the globe were experiencing delays of weeks or even months in withdrawing funds. Obviously, the exchange's problems with the U.S. government were continuing to create problems between Mt. Gox and the banking system.

Mt. Gox aside, there were several instances of major Bitcoin theft throughout the year. In April, Instawallet, a provider of web-based Bitcoin wallets, was hacked, resulting in the theft of more than 35,000 BTC, valued at more than $4.6 million. In October, Australian Bitcoin wallet provider Inputs.io was hacked for a loss of 4,100 BTC, worth more than $1 million. Also in October, a Bitcoin trading platform owned by Global Bond Limited simply vanished, taking Bitcoin worth more than $5 million with it.

On the good-news front, in July a project was initiated that linked Bitcoin with M-Pesa, a popular Kenyan mobile payments system, that promised to spur virtual online payments throughout Africa. In October, the first Bitcoin ATM was launched in Vancouver, British Columbia. And during the course of the year, several online and real-world merchants and services began accepting Bitcoin for payment, including OkCupid, WordPress.com, Reddit, Foodler, and Overstock.com.

Bitcoin was in the news again in October, when the FBI seized roughly 26,000 BTC from the Silk Road website. This was part of an investigation into Silk Road's alleged illegal activities; the site was well known as a marketplace for illegal drugs, with the virtually untraceable Bitcoin as the currency of choice. It wasn't the best kind of publicity for the fledging virtual currency.

Also not good was the news from China. On December 5, the People's Republic of China announced that it was prohibiting Chinese banks from using Bitcoins, and that Bitcoins could not be used as legal tender. It didn't ban individuals from trading Bitcoins as a commodity, but it did impose new reporting constraints.

All that said, the biggest Bitcoin news of 2013 had to be the huge increase in value at the end of the year. The exchange rate was approximately $140/BTC at the beginning of October, hit $200/BTC on November 3, skyrocketed to $900 on November 19, and hit an all-time high of $1,216/BTC on November 28.

That looked like a bubble, and it was. In December, the price crashed down to $600/BTC, rebounded back to $1,000/BTC, then fell again to $500/BTC, and ended the year in the $650/BTC range. If you held any Bitcoin during that period, it was a wild ride.

2014: Mt. Gox...and Beyond

The Bitcoin exchange rate remained volatile during the first few months of 2014, rising to $1,000/BTC in January, sinking to the $600/BTC range in February, and then hovering in the $400 to $500/BTC range for the next several months.

This volatility was due in part to the problems befalling Mt. Gox, once the largest Bitcoin exchange in the world. Continued issues with the U.S. government hindered its operations, as did poor business practices and ongoing technical and security issues.

Mt. Gox's website, in better days.

On February 7, 2014, Mt. Gox announced that they were halting all withdrawal requests while they obtained "a clear technical view of the currency processes." On February 10, the company stated that the current issue was due to a "bug in the Bitcoin software that makes it possible for someone to use the Bitcoin network to alter transaction details to make it seem like a sending of Bitcoins to a Bitcoin wallet did not occur when in fact it did occur. Since the transaction appears as if it has not proceeded correctly, the Bitcoins may be resent. Mt. Gox is working with the Bitcoin core development team and others to mitigate this issue."

To give you an idea of the magnitude of Mt. Gox's problems, a February poll indicated that 68% of the exchange's customers were currently awaiting funds they had requested withdrawn. The median waiting time was between one and three months, with 21% of customers waiting for three months or more. (Imagine waiting three months for your local bank to process a withdrawal!)

On February 23, Mt. Gox's CEO resigned and the company deleted all posts from their Twitter feed. The next day, Mt. Gox officially suspended all trading and, just hours later, its website went offline. Then the bomb dropped: On February 20, Mt. Gox filed for bankruptcy protection. It listed its liabilities at 6.5 billion yen (approximately $64 million), and its assets at just 3.8 billion yen.

As to the cause of all these problems, the company claimed to have lost close to 750,000 of its customers' Bitcoins, and 100,000 or so of its own store. The "lost" Bitcoins were worth around $473 million—not an insignificant amount.

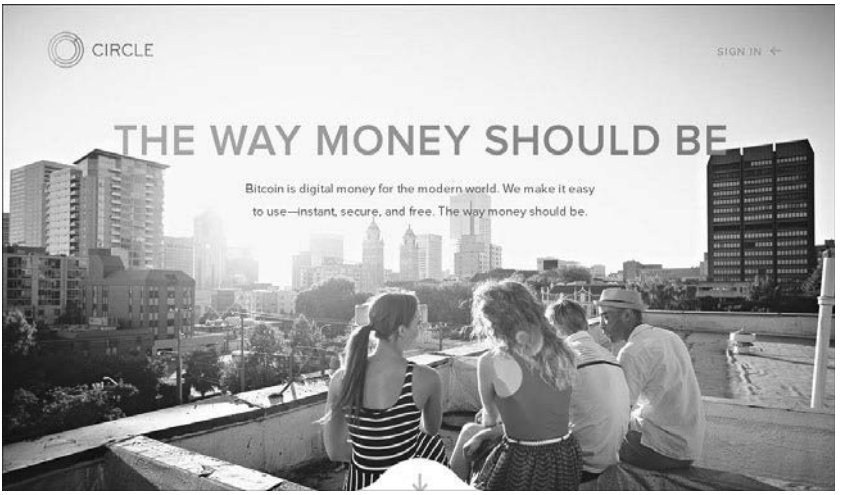
What happened to all those virtual funds? Mt. Gox released a statement that said, in part, "The company believes there is a high possibility that the Bitcoins were stolen." By hackers, presumably. The company's recently resigned CEO said that technical issues opened the door for those fraudulent withdrawals.

(Keeping up-to-date, on March 20 the company reported that it had found some Bitcoins, worth around $116 million, in an old digital wallet from 2011. That reduces the number of total Bitcoins lost down to around 650,000.)

Obviously, hacks and fraud can totally destroy any unsecured Bitcoin exchange; that's why we have regulations and insurance for traditional financial institutions. Mt. Gox is the biggest example of this type of value-destroying fraud, but not the only one. Witness the Bitcoin exchange Flexcoin, which was hit by hackers on March 2, 2014, smack dab in the middle of the whole Mt. Gox thing. The hack—and resulting losses—forced Flexcoin to shut up shop just one day later, stating, "As Flexcoin does not have the resources, assets, or otherwise to come back from this loss, we are closing our doors immediately."

March also saw the Internal Revenue Service rule that Bitcoin is not a currency, but rather an asset. This means that Bitcoin transactions should be taxed as capital gains, the same as stocks and other securities. This ruling could be troublesome for those wanting to use Bitcoin as a currency rather than an investment.

That said, the IRS ruling obviously had little impact on a Bitcoin start-up named Circle that launched on May 16. Circle's website enables consumers to purchase Bitcoin in any amount they choose and then spend their Bitcoin on online shopping and at real-world merchants and restaurants. Even better, Circle's Bitcoin exchange services come with all the safeguards that protect traditional currency transactions in the real world—and with no fees for deposits, withdrawals, or Bitcoin storage.



Circle—a new way to trade Bitcoin?

The same week, Halsey Minor, the founder of CNET, launched another new Bitcoin market dubbed Bitreserve. Funds held by members are backed by a full reserve of real-world currencies, including dollars, euros, yuan, yen, and pounds. The goal is to give members all the traditional values of a virtual currency but with more security and less value-destroying volatility.

Bitcoin Today

That's where things stand as of mid-year 2014, when this book was written. The whole Bitcoin industry (yes, it's now an industry) is still reeling from the Mt. Gox debacle, but also claiming that it's an isolated incident that had more to do with Mt. Gox's poorly run business than it did with any intrinsic flaw in the Bitcoin model. Bitcoin's price continues to hover in the $500 to $600/BTC range, nowhere near the inflated highs of late 2013. In fact, the currency looks downright stable compared to how it has been in the past.

Despite the turmoil, more and more merchants—both online and in the real world—are announcing that they will accept Bitcoin as payment for their goods and services. We're talking merchants as diverse as Digital River, which handles $30 billion/year worth of online transaction processing for digital software downloads, and Expedia, the big-time online travel site. Even eBay's PayPal says that they're "actively considering" integrating Bitcoin into the PayPal payment system, and it's rumored that several large financial institutions might be getting into the Bitcoin exchange business. Legitimacy appears to be near.

It has been an interesting six years or so, with Bitcoin rising from one man's idea to a viable world currency. Who knows where things will be six years from now?

Index

C

D

E

F

G

H

I

O

P

Q

R

S

T

U

V

W

X-Y-Z