LEARNING MADE EASY

2nd Edition

Cryptocurrency Mining for dummies

A Wiley Brand

Discover the process of mining new cryptocurrency

Learn the tech tools needed to handle crypto transactions

Join a mining pool and benefit from coin mining

Peter Kent

Tyler Bain

Coauthors of *Bitcoin For Dummies,* 2nd Edition

Cryptocurrency Mining

2nd Edition

by Peter Kent and Tyler Bain

for dummies®
A Wiley Brand

Cryptocurrency Mining For Dummies®, 2nd Edition

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Published simultaneously in Canada

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

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

Library of Congress Control Number: 2022938471

ISBN 978-1-119-88536-8 (pbk); ISBN 978-1-119-88537-5 (ebk); ISBN 978-1-119-88538-2 (ebk)

Table of Contents

Introduction

Welcome to *Cryptocurrency Mining For Dummies.* We're here to help you enter the wonderful world of cryptocurrency mining. Of course, you don't need our help. You can just go to Google or some other major search engine, search, and jump right in. You'll find plenty of information to help you!

Hah! Try it and see. It'll be like drinking from the proverbial firehose — you'll drown in a flood of confusing blog posts, conflicting "news" articles, unintelligible wiki articles, misleading YouTube videos. . . .

So that's where we come in. Our job is to break it all down into intelligible, easy-to-digest, bite-sized pieces that ordinary folk like yourself can read and understand.

About This Book

This book explains, simplifies, and demystifies the world of cryptocurrency mining. You find out what you need to know and do in order to decide if and how you're going to begin cryptocurrency mining.

In this book, we explain

- How cryptocurrency mining works, and what it's *for* (it can't *just* be a way for you to make money, right?)
- The different algorithms and how they function — Proof of Work, Proof of Stake, Delegated Proof of Stake, and more — and what hashing is all about
- The different types of mines: pool mining, solo mining, cloud mining
- The different types of hardware: CPU mining, GPU mining, FGPA mining, and ASIC mining
- How to pick the right cryptocurrency to mine
- How to find and work with a pool mining service

- How to set up your mining hardware and software
- How to calculate your potential earnings (or losses!), taking into account network hash rate, your mining rig's hash rate, currency exchange rate, the price of electricity, and so on
- Where to find a plethora of helpful resources to guide you on your cryptocurrency mining journey
- And plenty more!

Foolish Assumptions

We don't want to assume anything, but we have to believe that if you're reading this book, you already know a few things about the Internet and cryptocurrency. We assume that you understand how to work online and work with personal computing equipment. We also assume that you know how to buy and sell cryptocurrency, how to work with exchanges and wallets, and how to keep it safe.

This alone is a complicated subject, which would take an entire book to explain. It is essential that you understand these basics; this book focuses on a more advanced subject, cryptocurrency mining, and we just don't have room to cover these basics. We recommend you check out Peter's 8-hour online video course, which you can find at `CryptoOfCourse.com`; but one way or another, it's essential that you learn how to work with cryptocurrency safely, in a way that protects you from theft and loss.

Icons Used in This Book

This book, like all *For Dummies* books, uses icons to highlight certain paragraphs and to alert you to particularly useful information. Here's a rundown of what those icons mean:

TIP

A Tip icon means we're giving you an extra snippet of information that may help you on your way or provide additional insight into the concepts being discussed.

REMEMBER

The Remember icon points out information that is worth committing to memory.

TECHNICAL STUFF

The Technical Stuff icon indicates geeky stuff that you can skip if you really want to, although you may want to read it if you're the kind of person who likes to have the background info.

WARNING

The Warning icon helps you stay out of trouble. It's intended to grab your attention to help you avoid a pitfall that may harm your website or business.

Beyond the Book

In addition to what you're reading right now, this product also comes with a free access-anywhere Cheat Sheet that covers a variety of useful facts, such as background information on commonly mined cryptocurrencies, coin divisibility, popular pool mining services, and so on. To get this Cheat Sheet, simply go to `www.dummies.com` and enter **Cryptocurrency Mining For Dummies Cheat Sheet** in the Search box.

For information on Peter's *Crypto Clear: Blockchain & Cryptocurrency Made Simple* video course, visit `www.CryptoOfCourse.com`.

Where to Go from Here

As are all good reference tools, this book is designed to be read when needed. It's divided into several parts: cryptocurrency background and basics; mining-related foundational information; how to get started in cryptocurrency mining; the economics of mining; and the Part of Tens. We recommend that you start at the beginning and read through sequentially, but if you just want to know how to find pool mining services, read Chapter 7. If you need to understand how to calculate what equipment you would need to mine a particular cryptocurrency, read Chapter 11. If all you need is to understand the different forms of mining, Chapter 4 is for you.

However, cryptocurrency is a complex subject, and cryptocurrency mining more so. All the topics covered in this book are interrelated. We strongly recommend that you read everything in this book before you begin mining; it's essential that you have a strong understanding of everything involved before you begin. After all, your money is at stake!

1 Getting Started with Cryptocurrency Mining

IN THIS PART . . .

Review the basics of cryptocurrency.

Get acquainted with cryptocurrency mining.

Understand the blockchain and hashing.

Get to know the different forms of mining.

IN THIS CHAPTER

- Discovering digital currency
- Working with blockchain
- Hashing blocks
- Understanding public-key encryption
- Signing messages with the private key

Chapter 1

Cryptocurrency Explained

You may be eager to get your mining operation started, but before you can create cryptocurrency, we want to make sure you understand what cryptocurrency actually is.

The cryptocurrency thing is so new — or at least, most of the interest in cryptocurrency has occurred recently, even though cryptocurrencies of various forms have been around since the 1980s — that most people involved have a rather shaky understanding of what cryptocurrency is and how it works. The average cryptocurrency owner, for example, may not know what they own.

In this chapter, we review the history of cryptocurrency and how the different components function together. You'll have a better foundation to understand how to mine cryptocurrencies if you understand what it is.

A Short History of Digital Dollars

Cryptocurrency is just one type of digital currency . . . a special type. At the end of the day cryptocurrency may be thought of as a form of digital currency.

So, what's *digital currency,* then? Well, digital currency is a very broad term that covers a variety of different things. But in a general sense, it's money that exists in a digital form rather than tangible form (think coins and banknotes). You can transfer digital currency over an electronic network of some kind, whether the Internet or a private banking network.

TIP

In fact, even credit card transactions may be thought of as digital currency transactions. After all, when you use your credit or debit card at a store (online or off), the money is being transferred electronically; the network doesn't package up dollar bills or pound notes and mail them to the merchant.

First, take the Internet

The cryptocurrency story really all begins with the Internet. Digital currencies existed before the Internet was in broad use, but for a digital currency to be useful, you need, well, some kind of digital transportation method for that currency. If almost nobody is using a digital communications network — and until 1994 very few people did — then what's the use of a digital currency?

But after 1994, millions of people were using a global, digital communications network — the Internet — and a problem arose: How can you spend money online? Okay, today the answer is pretty simple: You use your credit cards, debit cards, or PayPal account. But back in the mid-90s, it was more complicated.

Add credit card confusion

Back in the mid-90s, some of you may recall (and many of you were too young back then to remember this, I realize), people were wary of using credit cards on the Internet. When I had my own publishing company and was selling books through my website in 1997, I (Peter — Tyler's too young to remember 1997) would often receive printouts of my website product pages in the mail, along with a check to pay for the book being purchased. I was taking credit cards online, but many people simply didn't want to use them; they didn't trust the Interwebs to keep their plastic safe.

In addition, setting up a payment gateway for credit cards was difficult and expensive for the merchant. These days, it's a pretty simple process to add credit card processing to a website — it's built into virtually all ecommerce software, and with services like Stripe and Square lowering the barriers of entry, getting a *merchant account* is no longer the huge hassle and expense it used to be.

Of course, we're talking commercial transactions here, but what about personal transactions? How can someone send a friend the money they owe, or how can a parent send beer money to their child away at college? (I'm talking PPP . . . pre-PayPal and web-based transfers between bank accounts.) If we were going to live in a digital world, surely we needed digital money.

REMEMBER

One important characteristic of cash is that cash transactions are essentially anonymous — there's no paper trail or electronic record of the transaction taking place. Plenty of people thought an equivalent form of anonymous or pseudonymous digital currency would be a vast improvement over traditional settlement methods.

So, many people thought there had to be a better way. We needed a digital currency for a digital world. These days, perhaps that viewpoint seems naïve; looking back it was obvious that the credit companies weren't going to see trillions of dollars of transactions shifting online and just wave goodbye! They wanted a piece of the action, unwilling to give up their monopoly, and so today, the primary transaction methods in the United States and most of Europe are bank cards of various kinds.

Add a dash of David Chaum

In the mid-1990s, people were streaming online and for various reasons many didn't want to, or couldn't, use credit cards (see preceding section). Checks were even more difficult (unless you wanted to mail it), and cash was out of the question. (Though — and here's a joke for the older geeks among you — I do recall a friend telling me to UUENCODE the $10 I owed him and email it to him. Again, this is Peter talking; I'm betting Tyler is too young to know what UUENCODE is.)

But back in 1983, a guy called David Chaum had written a paper called "Blind Signatures for Untraceable Transactions." Chaum was a cryptographer (someone who works with cryptography) and professor of computer science. His paper described a way to use cryptography to create a digital-cash system that could enable anonymous transactions, just like cash. (Modern cryptography is the science of securing online communications; we'll come back to this later.) In fact, Chaum is often referred to as the Father of Digital Currency as well as the Father of Online Anonymity.

Result? DigiCash, E-Gold, Millicent, CyberCash, and More

Bring together the Internet, complicated online transactions, a fear of using credit cards online, a desire for cash-like anonymous online transactions, and David Chaum's work in the '80s (see preceding section), and what do you end up with?

You get DigiCash, for a start, David Chaum's 1990 digital-cash system. Unfortunately, Mr. Chaum seems to be early for the party too often, and DigiCash was out of business by 1998. There was also E-Gold, a digital cash system supposedly backed by gold, DEC's Millicent (yes, yes, most of you are too young to remember DEC, too. . . . I'm starting to feel old writing this "historical" section), First Virtual, CyberCash, b-money, Hashcash, eCash, Bit Gold, Cybercoin, and many more. There was also Beenz, with $100 million in investment capital; Flooz, endorsed by Whoopi Goldberg (no, really!); Liberty Reserve (shut down after being accused of money laundering); and China's QQ Coins.

With the exception of QQ Coins, still in use on Tencent's QQ Messaging service, all these digital currencies are gone. Notably, many of these early digital currencies were in one way or another centralized with a trusted third-party intermediary.

Digital currency was not over, though. It got off to a rough start, with much trial and error, but plenty of people still thought that the world needed cash-like (in other words, anonymous) online transactions. A new era was about to begin: The cryptocurrency era.

The earlier digital currencies also depended on cryptography, it's true, but they were never known as cryptocurrencies. It wasn't until cryptocurrency was combined with a blockchain in 2008 that the term cryptocurrency started to gain usage, and the term really didn't begin to appear widely until around 2012. (Blockchain? It's a special form of database, but we'll describe in more detail later in this chapter.)

The Bitcoin white paper

In 2008 Satoshi Nakamoto published and posted in a cryptography forum known as the "Cypherpunk Mailing List" a document titled "Bitcoin: A Peer-to-Peer Electronic Cash System," saying, "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party," he said.

The following list of attributes, Nakamoto stated, were key to Bitcoin:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof of work.
- The proof of work for new coin generation also powers the network to prevent double spending.

The document is a fairly dry read, but it's worth spending a few minutes checking it out. You can easily find it by navigating to `https://bitcoin.org/bitcoin.pdf`. The abstract for the Bitcoin white paper begins with the following statement: "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution," Nakamoto wrote. He explains that his method has solved the "double-spending" problem, an issue plaguing earlier digital currencies: the challenge was to make sure that a digital currency couldn't be spent twice.

Nakamoto also describes using blockchain functionality, although the term blockchain appears nowhere in the white paper:

> We propose . . . using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

Bitcoin: The first blockchain app

Early in January 2009, Nakamoto launched the Bitcoin network into action, using blockchain (a concept that had been around since the early 1990s, though this was the first time it had been correctly implemented), and created the first block in the blockchain, known as the *genesis* block.

This block contained 50 Bitcoin, as well as the text *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* as a justification and explanation as to why a system like Bitcoin was so important. Nakamoto continued coding updates into the protocol, running a node, and potentially mined around a million Bitcoin, a number that would make him one of the richest people in the world by the end of 2017 (at least "on paper").

By the end of 2010, Satoshi Nakamoto published his last forum post and officially signed off from the project, but by this time many other cryptocurrency enthusiasts had joined in, began mining, supporting open source code development, and the rest is history.

Who (or what) is Satoshi Nakamoto?

So, who was this Satoshi Nakamoto guy . . . or gal . . . or organization? Nobody knows. Satoshi Nakamoto doesn't seem to be a real name; it's most likely a pseudonym. And if anyone knows for sure who Nakamoto really is, they're not saying. It's the great mystery of cryptocurrency.

There is a Japanese American man named Dorian Prentice Satoshi Nakamoto, born Satoshi Nakamoto apparently. This person was a trained physicist, systems engineer, and a computer engineer for financial companies — perhaps he was the Satoshi Nakamoto. However, he's denied it several times.

How about Hal Finney, who lived just a few blocks from Dorian Prentice Satoshi Nakamoto's home? He was a pre-Bitcoin cryptographer and one of the first people to use Bitcoin and claims to have communicated via email with the founder of Bitcoin. Some people have suggested he "borrowed" Satoshi Nakamoto's name and used it as a pseudonym.

Then there's Nick Szabo, who has long been involved in digital currency and even published a white paper on bit gold, before Nakamoto's Bitcoin white paper. Or what about Craig White, who at one point claimed to be Nakamoto, but was later accused of fraud? Or Dr. Vili Lehdonvirta, a Finnish economic sociologist, or Michael Clear, an Irish graduate student in cryptography, or the three guys who filed a patent that included an obscure phrase ("computationally impractical to reverse") also used in the Nakamoto Bitcoin white paper, or Japanese mathematician Shinichi Mochizuki, or Jed McCaleb, or some type of government agency, or some other kind of team of people, or Elon Musk, or, well, nobody knows, but theories abound.

The second biggest Bitcoin mystery? Nakamoto owned around a million Bitcoin, which in December 2017, was worth about 19 or 20 billion dollars. The entirety of Nakamoto's estimated Bitcoin fortune has not been moved or spent; why hasn't he touched this money?

What's the Blockchain?

In order to understand cryptocurrency, you need to understand a little about blockchains. Blockchain technology is complicated, but that's okay — you don't need to understand everything. You just need to know the basics.

Blockchains are types of databases. A *database* is simply a collection of structured data. Say that you gather together a bunch of names, street addresses, email addresses, and phone numbers and type them into a word processor. That's not a database. That's just a jumble of text.

But say that you enter that data into a spreadsheet. The first column is the first name, the second is the person's last name, and then you have columns for the email address, phone number, street address, city name, zip code, country, and so on — that's structured data. That's a database.

Most people use databases all the time. If you use some kind of financial management program, such as QuickBooks, Quicken, or Mint, your data is stored in a database. If you use a contact management program to store contact information, it's stored in a database. Databases, behind the scenes, are an integral part of modern digital life.

Blockchain around the world — the blockchain network

The blockchain is a database; it stores information in a structured form. You can use blockchains for many different purposes: for example, for *property rights registries* (who owns this piece of land, and how did they come to own it?), or *supply chain tracking* (where did your wine or fish come from, and how did it get to you?). Blockchains can store any kind of data. In the case of cryptocurrencies, though, blockchains store transaction data: who owns what amount of cryptocurrency, who gave it to them, and who have they given it to (how have they spent it)?

Of course, blockchains have several special characteristics. Firstly, they are networked. There is a Bitcoin network, a Litecoin network, an Ethereum network, just like there's an email network or a World Wide Web network.

Bitcoin, for example, is a network of thousands of nodes or servers, spread across the entire planet.

These nodes each contain a copy of the Bitcoin blockchain, and they communicate with each other and stay in sync. They use a system of *consensus* to come to an agreement regarding what the current, valid blockchain database looks like. That is, they all contain a matching copy of the blockchain.

Hashing: "Fingerprinting" blocks

Having the blockchain duplicated across many different computers is powerful, making it much harder to hack or manipulate. But there's something else that's also powerful: *hashing*. A *hash* is a long number that is a kind of fingerprint for data. The blockchain uses it as follows:

1. **A computer running a node gathers and validates Bitcoin transactions (records of Bitcoin sent between addresses within the blockchain) that are going to be added to the blockchain.**
2. **When the computer has collected enough transactions, it creates a block of data and *hashes* the data — that is, it passes the data to a special hashing algorithm, which passes back the hash.**

   Here's an example of a real-life hash, from a block in the Bitcoin blockchain:

   ```
   000000000000000000297f87446dc8b8855ae4ee2b35260dc4af61e1f5eec579Th
   ```

   A *hash* is a fingerprint for the data, and thanks to the magic of complex mathematics, it can't possibly match any other set of data. If the hashed data is changed even slightly — a 0 changes to a 5, or an A is changed to a B — the hash fingerprint will no longer match the original data.
3. **The hash is added to the block of transactions.**
4. **The block is added to the blockchain.**
5. **More transactions are collected for the next block.**
6. **After a full block of transactions is ready, the hash of the previous block is added to the current block.**
7. **The block — the transactions and previous-block's hash — are hashed again.**
8. **The process repeats, creating a timestamped chain of blocks.**

So, every block contains two hashes: the previous block's hash and the current block's hash, which is created by hashing the combination of all the Bitcoin transactions and the previous block's hash.

That's how blocks are chained together into the blockchain (see Figure 1-1). Each block contains the previous block's hash — in effect, a copy of the previous block's unique fingerprint. Each block is also, in effect, identifying its position in the blockchain; the hash from the previous block identifies the order in which the current block sits.

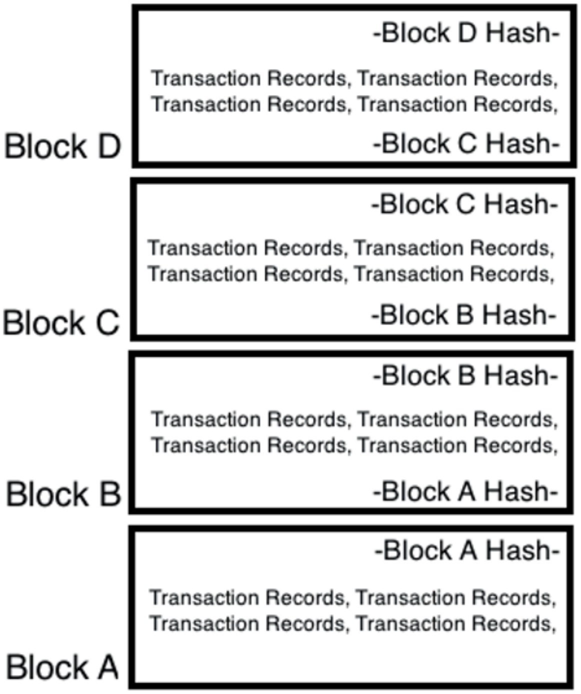
-Block D Hash-
Transaction Records, Transaction Records, Transaction Records, Transaction Records,
-Block C Hash-
Block D
-Block C Hash-
Transaction Records, Transaction Records, Transaction Records, Transaction Records,
-Block B Hash-
Block C
-Block B Hash-
Transaction Records, Transaction Records, Transaction Records, Transaction Records,
-Block A Hash-
Block B
-Block A Hash-
Transaction Records, Transaction Records, Transaction Records, Transaction Records,
Block A

FIGURE 1-1: Each block's hash is stored in the next block of data. The hashes chain the blocks together in an orderly fashion.

Blockchain is "immutable"

You may have heard that the blockchain is virtually *immutable*, which simply means that it can't easily be changed. If the Bitcoin blockchain says you own *x* Bitcoin, then you do own *x* Bitcoin, and there can be no disagreement . . . and nobody can go into the blockchain and hack it or somehow change or mutate it.

Imagine what would happen if someone went into a block (we'll call it Block A) and changed a little bit of data — for example, they go in and show that instead of sending someone 1 Bitcoin you sent 9 Bitcoin.

Well, the hash in Block A would no longer match its data. Remember, a hash is a fingerprint that identifies the data, so if you change the data, the hash no longer matches.

Okay, so the hacker could rehash Block A's data and then save the "corrected" hash. But wait, now the next block (Block B) would not match because Block B is carrying Block A's hash. So now say the hacker changes the Block A hash stored in Block B.

But now Block B's hash doesn't match Block B's data, because that hash was created from a combination of Block B's transaction data and Block A's hash!

So, Block B would have to be re-hashed, and the hash updated. But wait! That means Block B's hash stored in Block C now doesn't match!

See where we're going? This would ripple through the entire blockchain. The entire blockchain is now broken, by just modifying one single character in a block lower down. In order to fix the problem, the entire blockchain has to be recalculated. From the hacked block onwards, it must be "re-mined." What may look like a simple hack and database edit now turns into a major computational headache that cannot be easily completed.

So, this hashing function, combined with the fact that thousands of other nodes must be in sync with identical copies of the blockchain, makes the blockchain virtually immutable; it simply can't be easily hacked.

Nobody can change it or destroy it. Hackers can't get into the peer-to-peer node network and create transactions in order to steal crypto, governments can't close it down (China, for example, could attempt to shut down Bitcoin within its borders, but the blockchain would continue to exist in many other countries), a terrorist group can't destroy it, one nation can't attack another and destroy its blockchain, and so on. Because there are so many copies of the blockchain, and as long as enough people want to continue working with the blockchain, it's practically immutable and indestructible.

Where's the Money?

You may be wondering, "So where is the cryptocurrency? Where's the money?" Or perhaps you've heard of cryptocurrency wallets and think that's where the money is stored. Wrong. There's no money in a cryptocurrency wallet. In fact, there is no cryptocurrency.

Cryptocurrency blockchains are often described as ledgers. A *ledger* is described by Google Dictionary as "a book or other collection of financial accounts of a particular type." Ledgers have been around for hundreds of years, used to record transactions for individuals, businesses, government departments, and so on. The statement you get from your bank account or credit card is a form of ledger, showing you your individual transactions; money you pay to others, and money you receive from others.

FINDING THE BALANCE IN THE BLOCKCHAIN

Well, okay, the blockchain doesn't actually store a balance for each address. Nowhere in the blockchain does it state how much of the cryptocurrency any particular owner owns or how much any particular address has associated with it. Rather, you can use a blockchain explorer to follow all your transactions, incoming and outgoing, and the blockchain explorer can figure out your balance based on those transactions.

In the context of cryptocurrency, the blockchain is a digital ledger recording cryptocurrency you send to others, and cryptocurrency you receive from others.

Think of it this way. Say that you're a little compulsive and like to keep a record of the cash in your pocket. You carry a notepad, to record every time you put money into your pocket and every time you spend it, and you calculate the current balance. That notepad is a kind of transaction ledger, right?

Cryptocurrency is very similar to this ledger of cash transactions . . . except there's no pocket. The blockchain is the ledger; it stores a record of every transaction (when you first purchased or were sent the cryptocurrency, when you spent it or sold it, and the balance you own).

But there's no pocket and no cryptocurrency sitting in storage somewhere. The blockchain is simply a series of "mythical" (or virtual) transactions stored in the ledger. No currency is being physically transferred; we simply update the record to state that currency has been transferred.

The ledger says you own cryptocurrency, so everyone can validate and accept that you own it. And remember, that ledger can't be edited after being solidified into the chain — it can't be hacked. (See the preceding section for more on this topic.) So if the ledger says you own, say, half a Bitcoin, then you absolutely do, and you can sell that half Bitcoin to someone else by modifying the ledger to say that they own it!

But what about the wallet? The wallet must store money, right? No, cryptocurrency wallets do not store cryptocurrency. They store private keys, public keys, and addresses. Private keys are the most important because they control the addresses with which your cryptocurrency is associated in the blockchain.

What's the Crypto in Cryptocurrency?

The *crypto* in cryptocurrency refers to cryptography. So, what exactly is cryptography?

According to The Oxford English Dictionary, cryptography is "the art of writing or solving codes." Wikipedia's explanation is more complicated and more digital: "The practice and study of techniques for secure communication . . . cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages."

The history of cryptography goes back at least 4,000 years. People have always needed to send secret messages now and then, and that's what cryptography is all about.

Today's cryptography, with the help of computers, is far more complicated than the ancient ciphers of the classical world, and it's used more extensively. In fact, cryptography is an integral part of the Internet; without it, the Internet just wouldn't work in the way we need it to work.

Almost every time you use your web browser, you're employing cryptography. Remember the little lock icon, shown in Figure 1-2, in your browser's Location bar?

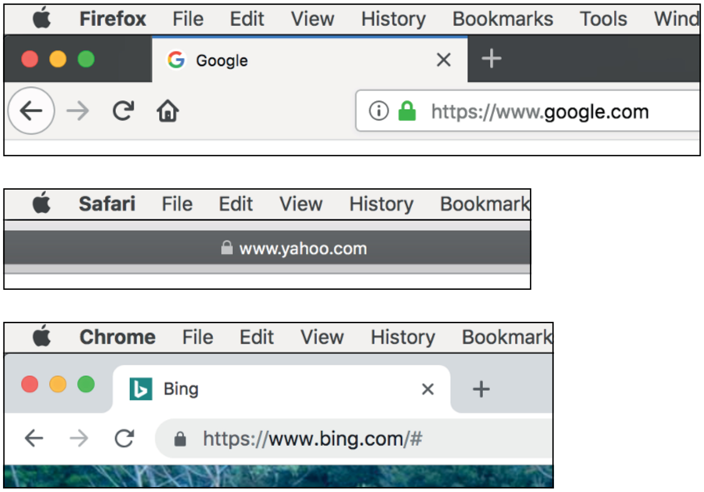
Firefox File Edit View History Bookmarks Tools Wind
Google
https://www.google.com
Safari File Edit View History Bookmark
www.yahoo.com
Chrome File Edit View History Bookmark
Bing
https://www.bing.com/#

FIGURE 1-2: Your browser's lock icon means that data submitted back to the web server will be encrypted with cryptography.