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

COPYRIGHTED MATERIAL

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.

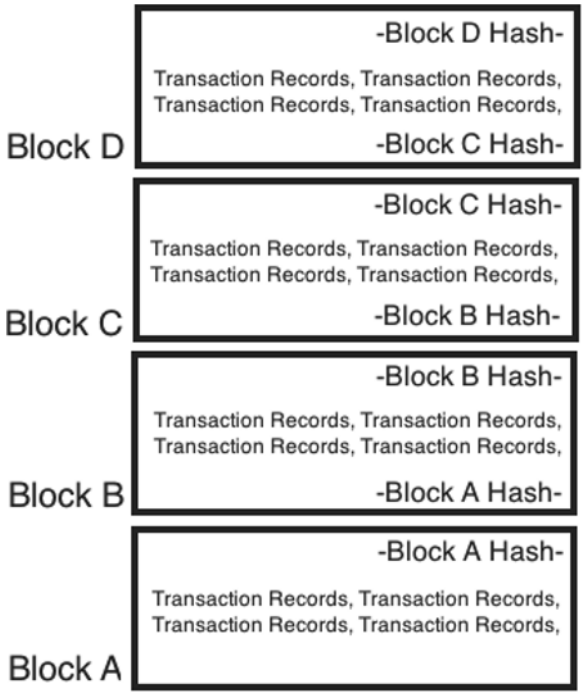

FIGURE 1-1: Each block's hash is stored in the next block of data. The hashes chain the blocks together in an orderly fashion.

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?

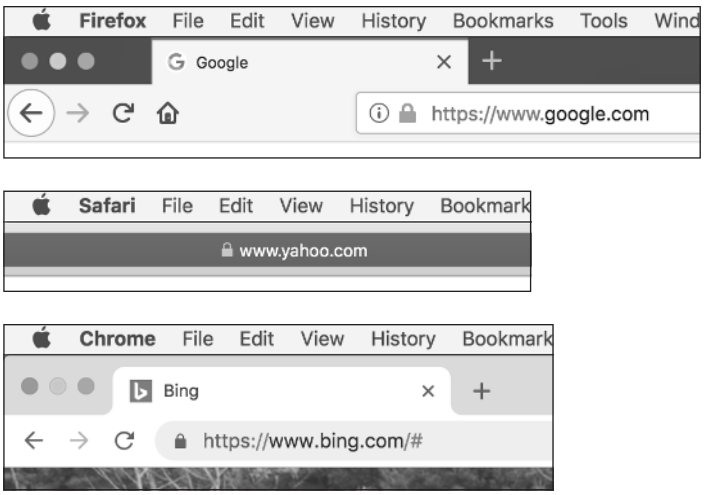

FIGURE 1-2: Your browser's lock icon means that data submitted back to the web server will be encrypted with cryptography.

The lock icon means the page is secured. When you send information to and from the browser to the web server and back, that information is going to be *encrypted* — scrambled — so that if it's intercepted on the hundreds or thousands of miles of Internet transmission between the two, it can't be read. When your credit card number is transmitted to an ecommerce site, for example, it's scrambled by your browser, sent to the Web server, and then unscrambled by the receiving server.

Ah, so, the blockchain is encrypted, right? Well, no. Cryptocurrency uses cryptography, but not to scramble the data in the blockchain. The blockchain is open, public, and auditable. Figure 1-3 shows you an example of a blockchain explorer designed for Bitcoin. Using a blockchain explorer, anyone can investigate the blockchain and see every transaction that has occurred since the genesis block (the first block of Bitcoin created).

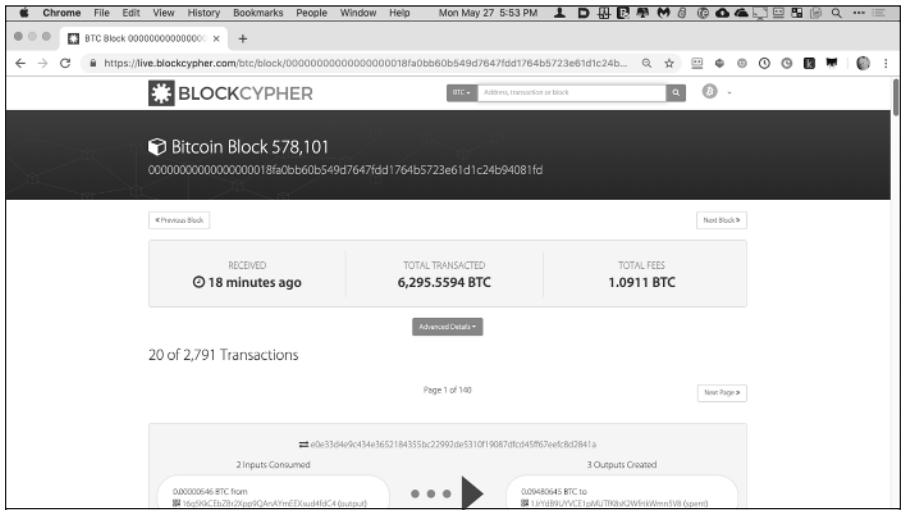

FIGURE 1-3: An example of a blockchain explorer tool, found at `https://live.blockcypher.com/btc`.

ENCRYPTED BLOCKCHAINS

You can build encrypted blockchains and encrypt data within a blockchain. For example, while the Bitcoin blockchain is unencrypted and open to inspection by anyone (see the blockchain explorer in Figure 1-3), it is still possible to create encrypted blockchains that obscure the transaction data, such as Zcash, but, in general, cryptocurrency blockchains are not encrypted, so anyone can read the transactions stored within them.

No, cryptocurrency isn't used to encrypt the data in the blockchain. It's used to sign messages that you send to the blockchain. These messages are the ones that trigger transactions and updates to the blockchain ledger.

Public Key Encryption Magic

Public key encryption is a clever little trick created using digital cryptography. And, by the way, this type of encryption is all accomplished using hugely complicated mathematics — the sort of mathematics that even most people with degrees in mathematics don't understand, the sort of mathematics that has names like *Carmichael numbers* and *Goppa codes*, the sort of mathematics that we certainly don't understand, and you don't either (well, most of you, dear readers, don't). But that's fine: Gravity isn't well understood either, but we all use it every day.

So, forget how this amazing stuff works, and consider instead what it is actually accomplishing. Now, imagine a safe, with two keyholes and two associated keys. One is a public key, and one is a private key. Now imagine that you put something into the safe and lock it using the public key. Once the door is closed and locked, the public key no longer has access to the safe; it can't be used to unlock the safe and extract the item. The private key, however, will work. The only way to open the safe is to use the private key.

In fact, this magical mathematical safe works both ways. You can lock it with the private key, but after you lock it, you can't use the private key to open the safe. Only the public key will open a safe locked with a private key.

Oh, and these two keys are magically associated. They work only with each other and no other keys. Private Key X will work only with Public Key X, and vice versa. You can't lock the safe with Public Key X and then unlock the safe with Private Key W or Private Key K, for example.

Okay, same principle, but now think of electronic messages. You can lock an electronic message with a public key — that is, you can use a key to scramble, or encrypt, the message. That message may be an email or information being sent from your browser to a web server.

After that locked (encrypted) message is received at the other end (the email recipient or the web server), only the private key can unlock it; the public key is useless at this point. And it must be the magically associated (okay, mathematically associated) key, and no other.

Encryption is a handy tool. It means I can give you a public key, and you can write me a message and encrypt it using the public key, and once encrypted nobody in the world can read it unless they have the private key. So, if I'm carefully protecting my keys, I'm the only person in the world who can read it.

The names of these keys aren't arbitrary. The private key should be truly private — only you, and nobody else in the world, should have access to it. The public key can be truly public. You can give it away. For example, if you want to have people email their messages to you, you can publish your public key — on your website, in the footer of your emails, on your business card, or whatever — so that anybody who wants to send a message to you can encrypt it with your public key knowing that you are the only person in the world who can read it (because you keep the private key secret).

TIP

How do you encrypt emails? Email encryption has been around for decades, but it simply never caught on with the public at large. Still, you can encrypt email from most email systems, such as Outlook, Gmail, and Yahoo! Mail, and there are systems, such as ProtonMail, that encrypt it by default.

This process is essentially what your web browser uses when you send your credit card information online; the browser uses the web server's public key to scramble the data so that only the web browser, with the associated private key, can decrypt and read the credit card information. (Okay, that's a simplification. Browser-to-server communication is more complicated than this description, involving temporary session keys, and so on; but the basic principle still applies.)

Messages to the blockchain

You use public-key encryption when you send transactions to the blockchain. When you want to send, say, Bitcoin, to someone else, you send an encrypted message to the blockchain saying "send *x.xx* of my Bitcoin to this address."

But wait. I just told you the blockchain isn't encrypted, and now I'm telling you the messages to the blockchain are encrypted! So why do you care if the message going to the blockchain is encrypted if you're just going to decrypt it anyway?

Well, remember I told you this lock/unlock thing works both ways. You can lock with the public key and unlock with the private key or lock with the private key and unlock with the public key. Either way, the data is scrambled. The difference is who has the ability to unscramble it. If you scramble something with the public key, the only person in the world who can unscramble it is the person with the

private key. But if you scramble it with the private key, the only person in the world who can open it is . . . everybody! Anybody and everybody can get to the public key. It's public, remember!

So, what's the purpose of encrypting a message with the private key? Not to secure it, obviously, because anybody can decrypt it. No, the purpose is to *sign* the message (transaction) and prove ownership of the associated public key.

Signing messages with the private key

Say that I publish my public key on my website, in my emails, and on my business cards. Now, one day you get a message that seems to come from me. But how can you be sure it's from me? Well, I encrypted the message using my private key. So, you take my public key (which is publicly available) and use it to decrypt the message. If the message really is from me, my public key will decrypt it, and you'll be able to read it. If it isn't, the decryption won't work, because it came from someone else.

So, by encrypting the message with the private key, I have in effect signed the message, proving that it came from me. The recipient knows that the message was created by the person holding the private key that is associated with the public key that opened the message up and made it readable.

The blockchain address — your money's home

All the cryptocurrency in the blockchain is associated with addresses. Here's one I just grabbed from the Bitcoin blockchain using the blockchain explorer at `blockchain.com`, for example:

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

Trillions of different address combinations are possible, so this address is fundamentally unique. Now, where did this address come from? It came from a wallet that generated it from the private key. That wallet contains a public key and a private key.

REMEMBER

The public key is associated with the private key; in fact, it's created from the private key. The address is associated with the public key; in fact, it's created from the public key. So, all three are mathematically, and uniquely, associated with each other.

Sending a transaction message

So, here's how cryptography is used when you want to send a transaction to the blockchain, to transfer a cryptocurrency balance to another person. Say there's an address in the blockchain with Bitcoin associated with it. When I checked, `1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq` had a balance of 0.10701382 Bitcoin. Now, say this is your Bitcoin, and you want to send, perhaps, 0.05 Bitcoin to a friend, an exchange, or a merchant from whom you are buying a good or service.

TIP

The address I use in this example is a real address; you can see it for yourself in a blockchain explorer. (Use this link to get to it: `https://blockstream.info/address/1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`.) At the time of writing, it had 0.10701382 Bitcoin. By the time you see it, the number may be different, of course.

You send a message to the blockchain saying, essentially, "I own address `1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`, and I want to send 0.05 Bitcoin to address `1NdaT7URGyG67L9nkP2TuBZjYV6yL7XepS`."

If I just sent a plaintext (unencrypted) message to the blockchain, there would be a huge problem of verification and validity. How would the Bitcoin node receiving this message know that I do indeed own this address and the money associated with it? I could just be spoofing this information and making this up, right?

What we do is use the wallet to sign the message using the private key associated with the address. In other words, we use the private key to encrypt the message. Then we take the public key, add it to the encrypted message, and send it all out across the cryptocurrency network.

MESSAGE TO THE BLOCKCHAIN

How do you send a message to the blockchain? That's what your wallet software does. In fact, wallet software is less like a wallet — your wallet contains no cryptocurrency — and more like an email program. Your email program sends messages across the email network. Your wallet sends messages (about transactions) across the cryptocurrency network.

Unraveling the message

So, the node — a computer containing a copy of the cryptocurrency blockchain — receives the message. It takes the public key that has been attached and decrypts the message. The node learns something: "This message must have been encrypted — signed — by the private key associated with the public key." Of course, that's not really saying much. It's virtually a tautology! By definition, if the public key can decrypt a message, the message must have been encrypted with the matching private key. Whoop-de-doo.

But remember, the public key is mathematically associated with the address `1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`. So now the node can examine the two, asking in effect "Is the public key associated with the address?" If the answer is yes, then the node also knows that the private key is associated with the address (all three are uniquely associated with each other). So, what does the node tell itself?

"This message, sending money from `1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`, was sent by the private key that was used to create this address . . . so the address must have been sent by the person who owns the address and therefore owns the money associated with the address."

TIP

I know this concept can be confusing; it's hard to "get your head around." So here's another way to think about it: The only person who could have sent an encrypted message with transaction instructions for this address along with the public key that originally created the address is the person controlling the associated private key — that is, the owner of the address and the money associated with it, thus verifying ownership and validating the transaction.

WHOEVER OWNS THE PRIVATE KEYS OWNS THE MONEY

Okay, so maybe there are more people with access to the key. But as far as the technology is concerned, it doesn't matter. Whoever has access to the private key has the cryptographic right to control the money assigned to the blockchain address associated with the key. You may hear the phrase "whoever has the private key owns the money" or "not your private key, not your Bitcoin." They may not have acquired it legitimately or legally own it, but they can control it nonetheless. So, protect your private keys!

PSEUDONYMOUS CRYPTOCURRENCIES

Some cryptocurrencies are more anonymous than others. Bitcoin, for example, is often termed *pseudonymous* because it's only partially anonymous. Imagine that someone subpoenas transaction records from an exchange and discovers that you purchased a couple of Bitcoin on the exchange and your identity was tied to those transactions via AML (anti-money laundering) and KYC (know your customer) data collection procedures required by law in the United States (and other countries). They'll have the address that the exchange used to store those Bitcoin, right? Well, now they can trace the transactions from that address through the blockchain using a blockchain explorer. And different addresses can be associated with each other in certain ways, so it would be possible for someone with the information — a tax authority, for example, or police agency — from a single starting point, to create a picture of a person's Bitcoin transactions. So, Bitcoin as it is commonly used today is not fully anonymous. Other currencies, such as Monero or Zcash, claim to get much closer to true anonymity. However, improvements to Bitcoin, such as conjoin and Layer 2, are likely to make Bitcoin more anonymous in the future.

So that's the crypto in cryptocurrency! You can control money in the blockchain anonymously through the use of cryptography, using public and private key pairs and associated addresses, by cryptographically signing messages.

The Basic Components of Cryptocurrency

The following sections take a look at how the basic components of cryptocurrency fit together.

What's in a wallet?

The *wallet* is where everything begins as far as your cryptocurrency is concerned. When you create a wallet file, the wallet software will create a private key. That private key is used to create a public key, and the public key is used to create an address. The address has never before existed in the blockchain and still doesn't exist in the blockchain yet.

After you have an address, you have a way to store cryptocurrency. You can give the address to someone from whom you're buying cryptocurrency or an exchange, for example, and they can send the cryptocurrency to that address — in other words, they send a message to the blockchain saying "Send *x* amount of crypto to

address *x*." Now the address exists in the blockchain, and it has cryptocurrency associated with it.

A *wallet program* is a messaging program that stores your keys and addresses in a wallet file. The wallet program does these primary things:

- It retrieves data from the blockchain about your transactions and balance.
- It sends messages to the blockchain transferring your crypto from your addresses to other addresses, such as when you make a purchase using your cryptocurrency.
- It creates addresses you can give to other people when they need to send cryptocurrency to you.

Private keys create public keys

The private key in your wallet is used to create the public key that is used to unencrypt your messages sent to the blockchain. Private keys must be kept private; anyone with access to the private key has access to your money in the blockchain.

Public keys create blockchain addresses

Public keys are also used to create addresses. The first time an address is used, someone's wallet software sends a message to the blockchain saying "Send *x* amount of cryptocurrency to address *x* from address *y*." Until this point, the address did not exist in the blockchain. After the wallet software has sent the message, though, the address is in the blockchain, and money is associated with it.

The private key controls the address

The private key controlling the address is a hugely critical concept in cryptocurrency, and people who lose access to their cryptocurrency, or have their cryptocurrency stolen, don't understand this (see Figure 1-4). In this book, we won't be going into detail about protecting private keys, but make sure you protect your private keys! Don't lose them and don't let other people discover them!

"FORKING" CRYPTOCURRENCIES

A *fork* occurs when one cryptocurrency splits into two. That is, the network nodes fall out of consensus, and a copy is made of the cryptocurrency software, a change is made to the copy, and the two different software sets then build separate blockchains Thus, for example, in January 2015, a copy of the DASH code, named DNET, was made. Both DASH and DNET then continued development as separate cryptocurrencies, and DNET was later renamed PIVX (Private Instant Verified Transaction).

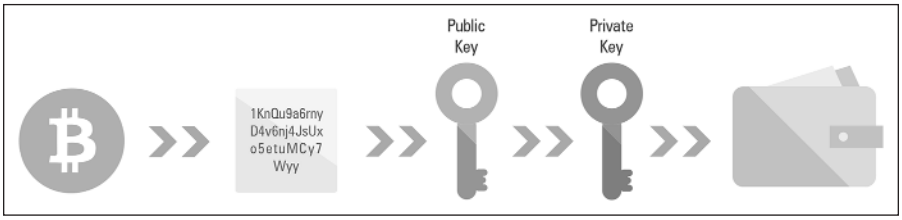

FIGURE 1-4: The cryptocurrency is associated with an address in the blockchain; the address is derived from the public key, which is associated with a private key . . . which is kept safe in a wallet.

Where Does Crypto Come From? The Crypto Mines (Sometimes)

So where does cryptocurrency come from? Cryptocurrency can be *mined* – the least common form, though the one you're evidently most interested in based on your interest in this book — or it can be *pre-mined*.

To say that a cryptocurrency has been *pre-mined*, or is *nonmineable*, simply means that the cryptocurrency already exists. The blockchain is a ledger containing information about transactions. When the blockchain was first created, the ledger already contained a record of all the cryptocurrency that the founders planned for. No more will be added; it's all there in the blockchain already.

In fact, although we hear a lot about cryptocurrency mining, the majority of cryptocurrencies (at the time of writing, more than 2,000 different flavors) are pre-mined: 74 or so of the top 100 cryptocurrencies are nonmineable, and overall, around 70 percent of all cryptocurrencies cannot be mined.

An example of a pre-mined currency is XRP, often known as Ripple, which is currently the second biggest cryptocurrency (in terms of *market capitalization* — that is, the value of all the cryptocurrency in circulation). XRP is stored within the RippleNet blockchain.

When the Ripple blockchain was created, 100 billion XRP were already recorded in the blockchain, although most had not been distributed. The founders of Ripple held 20 percent, and even now almost 60 percent of the currency is not in circulation.

Another example is Stellar, a payment network originally funded by the Stripe payment service, which at the time of writing was the fourth largest cryptocurrency. Stellar has a total supply of more than 100 billion lumens, 2 percent of which were assigned to Stripe for its investment.

So, no, not all cryptocurrencies can be mined (in fact, most can't). But that's not why you're reading this book, now, is it?

The good news, though, is that you can mine around 600 cryptocurrencies (though you'll never want to mine the vast majority). To decide which ones to mine, see Chapter 8.