1

WHAT IS BITCOIN?

In the simplest terms, Bitcoin is just another currency. The term *Bitcoin* refers to the entire currency system, whereas *bitcoins* are the basic units of the currency.[1] As with dollars, euros, yen, and gold coins, you can save bitcoins, spend them on goods and services, and exchange them for other currencies. However, Bitcoin is the world's first currency that is both digital and decentralized.

A *digital currency* is one that can be easily stored and used on a computer. By this definition, even dollars can be considered a digital currency, since they can be easily sent to others or used to shop online, but their supply is controlled by a centralized bank organization. In contrast, gold coins are *decentralized*, meaning that no central authority controls the supply of gold in the world. In fact, anyone can dig for gold, create new coins, and distribute them. However, unlike digital currencies, it's not easy to use gold coins to pay for goods (at least not with exact change!), and it's impossible to transfer gold coins over the Internet. Because Bitcoin combines these two

1. Similar to how *renminbi* is name of the Chinese currency, but the *yuan* is the basic unit.

properties, it is somewhat like digital gold. Never before has there been a currency with both these two properties, and its impact on our increasingly digital, globalized world may turn out to be significant.

Sometimes called a stateless currency, Bitcoin is not associated with any nation. However, you should not consider Bitcoin to be in the same category as *private* currencies, hundreds of which have existed in various forms in the past.[2] Private currencies, whether issued by a person, a company, or a nonstate organization, are centrally controlled and run the risk of collapse due to bankruptcy or other economic failure. Bitcoin is not a company, nor does a single person or organization issue or control bitcoins; therefore, it has no central point of failure. For this reason, nobody can inflate the currency supply and create hyperinflation crises, such as those that occurred in post–World War I Germany and more recently in Zimbabwe.[3]

Many people are asking about the motive behind the creation of Bitcoin, so let's explore the currency's purpose.

Why Bitcoin Now?

Until recently, people could not send *digital cash* back and forth to each other in a reliable way without a central mediator. A trusted central mediator such as PayPal can track payments and money transfers in a privately held account ledger, but it wasn't clear how a group of strangers who *do not* trust each other could accomplish the same transactions dependably.[4] Sometimes referred to as the Byzantine Generals' Problem, this fundamental conundrum also emerges in computer science, specifically in how to achieve consensus on a distributed network.

2. For example, in the mid-1800s, banks, companies, churches, and individuals issued hundreds of private currencies in the United States. Eventually, most of these private currencies lost all their value.

3. Between 1921 and 1924, the value of the German mark fell by a factor of more than 10 trillion due to overprinting by the government. In 2008, the government of Zimbabwe printed so much of its currency that in a single year, a loaf of bread increased from $1 to $100 billion. In both cases, any savings that people had in the form of national currency were completely destroyed.

4. To say that something is *decentralized* is more or less equivalent to saying that it is run by a group of strangers who don't necessarily trust each other.

In 2008, the problem was elegantly solved by Bitcoin's inventor, known pseudonymously as Satoshi Nakamoto. Satoshi's significant breakthrough made it possible for a digital currency to exist without relying on a central authority. Satoshi described the solution to the Byzantine Generals' Problem and the invention of Bitcoin in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." But the creation of the software that demonstrated the concept in practice was released a year later.

Although the first version of the software was written by Satoshi, it quickly became a community project as the software was improved and maintained by hundreds of volunteers. Currently, the software is open source, and anyone can read and contribute to it. In January of 2009, the first bitcoins were distributed using the early Bitcoin software, and since then transactions have been running smoothly. Slowly but surely, an increasing number of people have started using Bitcoin, and what began as an experiment is now a multibillion dollar economy that processes hundreds of thousands of transactions per day (and is growing quickly).

The Benefits of Using Bitcoin

Bitcoin is an inherently international currency; anyone can send bitcoins to anyone else in the world, in any amount, almost instantly. In addition, it is becoming increasingly possible to travel the world and spend bitcoins without having to change them into the local currency. Because no middleman is involved, transaction fees are negligible. Unlike with credit cards, which require giving online merchants your personal information, you can use bitcoins to shop online while maintaining your privacy. There is no risk of losing your savings due to runaway inflation because bitcoins were designed to have a fixed supply. Bitcoins are also fundamentally impossible to counterfeit.

As a merchant, you can start accepting bitcoins as payment immediately without filling out tedious paperwork (compared to setting up the credit card transaction process). You can also own bitcoins without anyone else knowing, and no third party or government can seize your money. (The privacy this feature entails may protect the security and freedom of political dissidents living under repressive regimes, for example.)

Thanks to all of its benefits, Bitcoin continues to increase in popularity; however, anyone familiar with Bitcoin will agree the technology behind it is difficult to explain and understand. At first blush, it's hard to grasp how bitcoins are stored, how they are used, or even where they come from.

The Complexity and Confusion of Bitcoin

Rarely do we get to see the creation of a new currency, let alone one that is so different from previous currencies. This creates major challenges in comprehension and comfort for most people.

Bitcoin can be compared to the advent of paper currency years ago when everyone was using gold and silver coins. Then, it must have seemed strange and confusing to attribute value to little pieces of paper instead of precious metals. Today, paper currency feels fairly safe, and trading paper for a purely digital asset like bitcoins seems odd. Furthermore, the economic and social consequences of switching to a decentralized digital currency are still unclear. Even Satoshi and the early volunteers who helped develop the concept could not have imagined precisely how Bitcoin would be used and valued by society, much as the creators of the Internet in the 1980s could not have predicted how transformative it would become.

Confusion also stems from the fact that Bitcoin is a truly complex technology. It relies not only on Satoshi's breakthrough to achieving consensus on a distributed network but also on modern cryptographic techniques, such as digital signatures, public/private key pairs, and secure hashing. (These cryptographic concepts are covered in detail in Chapter 7.) The

issuing of new currency occurs through a cryptographic lottery called mining that anyone can participate in. Mining simultaneously processes transactions made by Bitcoin users. To resist abuse from those who might want to destroy the network, Bitcoin's design uses game theory to align the incentives of those who maintain the network and those who want to act in their own selfish interest. (Bitcoin mining and game theory is explained in detail in Chapter 8.)

Put simply, you cannot learn and completely understand Bitcoin in a single afternoon. However, we hope this book will help you understand the basics of Bitcoin as quickly as possible.

What's in This Book?

To make sense of the Bitcoin technology and phenomenon, you must view it from multiple perspectives. This book is organized around those perspectives.

- First, we'll look at Bitcoin from the perspective of a basic user. In Chapters 2–4 we describe how Bitcoin works and how you can acquire, spend, and safely store bitcoins—so you can actually start using Bitcoin.
- Next, in Chapters 5 and 6, we take a philosophical perspective on Bitcoin. Chapter 5 is an adventure story told from the perspective of Crowley the cryptographer. Crowley gets stranded on an island and needs to figure out how to efficiently exchange goods with inhabitants of other distant islands. Crowley knows about Bitcoin from a chance encounter with Satoshi but has significant doubts about the currency. In the story, he works through his doubts (which may be similar to yours) by giving Bitcoin a chance.

  Chapter 6 continues in this philosophical vein by looking at the potentially broader impact of Bitcoin and the potentially uneasy relationship of Bitcoin and its users with nation states whose currencies compete with Bitcoin.
- Then, we'll look at Bitcoin from the perspective of an advanced user. Chapters 7–9 describe the cryptographic methods behind Bitcoin, the details of bitcoin mining, and the nuances of various third-party wallet software solutions.
- Finally, in Chapter 10, we'll look at what the distant future might look like in a world where Bitcoin has gone mainstream.
- For programmers and developers who are new to Bitcoin, the appendices show you how to write your own programs to send and receive bitcoins.

As you read this book, keep in mind just how new Bitcoin is as a technology. For fields like particle physics, Egyptian history, or constitutional law, we can turn to authority figures that have devoted the better part of their lives to studying those subjects; by comparison nobody is really an

expert on Bitcoin. Just as there were no electricians before the discovery of electricity or programming gurus before computers were invented, arguably no Bitcoin experts exist today. We are all Bitcoin beginners, and no one can predict with any clarity how Bitcoin will evolve, even a year or two into the future.

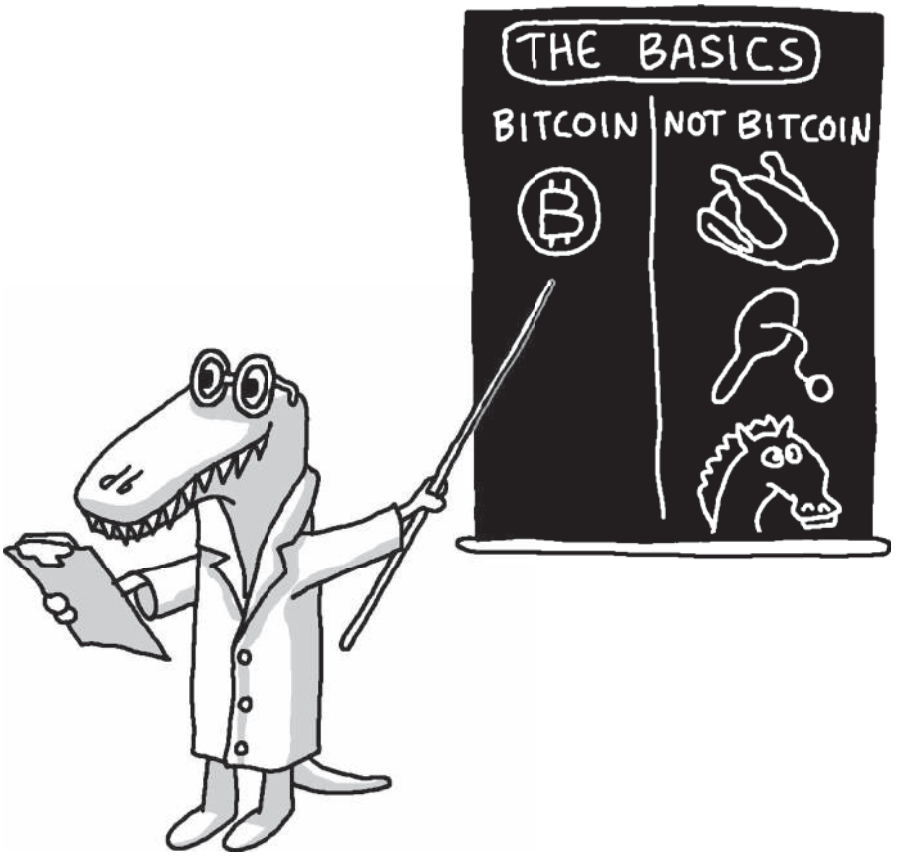
On the upside, this means that if Bitcoin becomes widely used in the future, the potential exists for *you* to become one of the early experts in Bitcoin, since you are studying this technology at such an early stage. We hope you will be inspired by the ideas behind Bitcoin and will make your own contributions to this wonderful technology in years to come.

Now, let's learn some Bitcoin basics.

2

BITCOIN BASICS

In our experience, the simplest way to get a person excited about Bitcoin is to have him purchase something with it. That's how we got hooked ourselves. In this chapter, we'll help you perform your first Bitcoin transaction, without worrying about too much technical stuff. Along the way, though, we'll discuss how Bitcoin works. After reading this chapter, you'll understand the basics of Bitcoin—enough to chat about it at any cocktail party.



How Bitcoin Works in Simple Terms

In the Bitcoin system, everyone cooperates to keep track of everyone else's money, and as mentioned in Chapter 1, no central authority (e.g., bank or government) is involved. To best understand how the system works, let's walk through an example using dollars first.

Imagine only $21 million exists in the world, and there also exists a detailed list of all the people who possess that money. Everyone, including you (even though you have only $5), has a copy of this list. When you give $2 to your friend, you must subtract $2 from your entry on the list and add $2 to her entry. After informing her of the transaction, she updates her list as well. In fact, everyone in the world needs to update the list; otherwise, the list would be inaccurate. Therefore, not only do you need to notify your friend, but you also need to publicly announce that you are updating the list. If you tried to cheat the system and send your friend $1000, your cheating attempt would be easy to catch because everyone knows you have only $5 to give.

Now, imagine that all transactions are carried out on computers that communicate via the Internet, and replace *dollars* with *bitcoins*. This is how Bitcoin works. Pretty simple actually. So why does Bitcoin seem so complex?

The answer is threefold: First is the tricky question of how the units of any new currency system (whether bitcoins or seashells) should be valued. Should a haircut be worth 5000 bitcoins or 0.005 bitcoins? Second, many small details are involved in implementing and using Bitcoin, even though the overall concept is fairly straightforward. For example, how do you obtain a copy of the list, and how are bitcoins initially distributed? Third, an entire lexicon of new and unfamiliar words (e.g., mining) is used in the Bitcoin world.

We'll leave the first point about the value of bitcoins for a later chapter. In this chapter, we'll address the last two points by explaining the major concepts used in Bitcoin, namely the Bitcoin address, the private key, the Bitcoin wallet, and the blockchain. We'll also briefly discuss Bitcoin mining and walk you through the process of receiving and sending your first bitcoins so you can see how the system works. But first, you need to understand the Bitcoin units in more detail.

Bitcoin Units

As explained in Chapter 1, Bitcoin refers collectively to the entire currency system, whereas bitcoins are the units of the currency. Although the total currency supply is capped at 21 million bitcoins, each one can be subdivided into smaller denominations; for example, 0.1 bitcoins and 0.001 bitcoins. The smallest unit, a hundred millionth of a bitcoin (0.00000001 bitcoins), is called a *satoshi* in honor of Satoshi Nakamoto. As a result, goods can be priced in Bitcoin very precisely, and people can easily pay for those goods in exact change (e.g., a merchant can price a gallon of milk at 0.00152374 bitcoins, or 152,374 satoshis).

Rather than writing the term *bitcoins* on price tags, merchants commonly use the abbreviated currency code *BTC* or *XBT*; 5 bitcoins would be written as 5 BTC. Despite the fact that the BTC abbreviation has been widely used since the beginning of Bitcoin's development, more recently some merchants and websites have started using XBT because it conforms better to certain international naming standards.[1] As bitcoins have appreciated in value, it has become increasingly common to work with thousandths or even millionths of bitcoins, which are called *millibitcoins (mBTC)* and *microbitcoins (μBTC)*, respectively. Many people have suggested simpler names for Bitcoin's smaller denominations, and one that has gained traction is referring to microbitcoins (quite a mouthful) as simply as *bits*.

1 bitcoin = 1 BTC or 1 XBT

1 BTC = 1,000 mBTC

1 mBTC = 1,000 μBTC

1 μBTC = 100 satoshis = 1 bit

1. The standard for currency codes (ISO 4217) uses the first character in the code to refer to the country issuing the currency. However, since Bitcoin is a nongovernmental currency, the standard suggests that its name should start with *X*, as is the case with gold or silver, whose codes are XAU and XAG, respectively.

Now that you know the terms for various Bitcoin units, you need to increase your Bitcoin vocabulary, so let's talk about what is meant by a Bitcoin address.

The Bitcoin Address

Bitcoin uses a public ledger that indicates the number of bitcoins and their owners at any given time. But instead of associating names of people with accounts, the ledger only lists *Bitcoin addresses*. Each address can be thought of as a pseudonym for a person (or group of people, business, etc.), and the use of pseudonyms is why people can use bitcoins without revealing personal information. The following is an example of a Bitcoin address:

```
13tQ1fbTMB6GxUJfMqCSDgivc8fvkHEh3J
```

Like a bank account number, a Bitcoin address consists of a string of letters and numbers (usually beginning with the number 1). To send bitcoins to others (e.g., an online merchant, a friend, or a family member), you only need to know their Bitcoin address. In turn, when you share your address with others, they can send you bitcoins. Because Bitcoin addresses are cumbersome to type, many people use *quick response (QR) codes* to represent their address (see Figure 2-1).[2] For convenience, you can put your Bitcoin address, either typed or as a QR code (or both), on your business card, personal website, or storefront (if you're a merchant). Although you need an Internet connection to *send* bitcoins, you don't need to be connected to *receive* them. For example, if you work for a charity and pass out thousands of business cards containing your Bitcoin address and a statement like "Please consider donating in bitcoins," your organization can collect bitcoins while you sleep.

Figure 2-1: QR codes can be used to represent arbitrary data. They are easy to scan with smartphones and so are convenient for sharing the long strings of characters used for Bitcoin addresses.

2. The QR code is just one of many ways to easily share a Bitcoin address. Another method is to use a *first bits* scheme in which you share only the first few characters of your Bitcoin address, which has been abbreviated by a Bitcoin address–shortening services (similar to a URL-shortening service). Starting with version 0.9 and later, Bitcoin also supports *human-readable* Bitcoin addresses that replace the traditional ones—much as a website address such as toys.com replaces the less user-friendly IP address of 123.100.101.111.

As you know, in traditional banking, moving money from one account to another means that the bank would update its privately held ledger that listed every account at that bank. If a fire or other disaster destroyed that ledger, information about who owned the assets at the bank might be lost forever. Although Bitcoin also uses a ledger, identical copies of it are distributed across millions of computers around the world. Consequently, no central point of failure exists, and transactions recorded on the Bitcoin ledger are permanent and impossible to erase. Moving bitcoins from one address to another is equivalent to sending an instruction to all of the computers on the Bitcoin network to update each ledger in the same way.

Because all transactions on the Bitcoin ledger are *public information*, maintaining privacy (if that is desired) can be a challenge. Although no personal information is on the ledger, if you share your Bitcoin address with your friends or post it in a public place that others can associate with your identity, your Bitcoin balance at that address will be known to everyone (including all incoming and outgoing transactions). To enhance your privacy, you can use many Bitcoin addresses but publicly share only some of them.[3]

So how do you move bitcoins from one address to another (i.e., spend them)? Well, this action requires a private key.

The Private Key

A *private key*, like a Bitcoin address, is a long string of numbers and letters (usually beginning with the number 5). As with Bitcoin addresses, QR codes are often used to represent private keys because of their length. Each private key is paired with a single Bitcoin address and is able to *unlock* the bitcoins at that address (i.e., move them elsewhere).[4] The following is an example of a private key:

```
5J2ae37Jwqzt7kSp9rE17Mi2LbkHXx4tzNSzbq7xDp2cQJCzhYo
```

Whereas a Bitcoin address is similar to a bank account number, a private key is more like a PIN: You need it to authorize a withdrawal or an expenditure. When a transaction is broadcast to the Bitcoin network, instructing bitcoins to be moved from one address to another, computers on the network check whether the transaction is authorized before making any updates to the public ledger. Specifically, they check whether the transaction has been *digitally signed* using a private key. A digital signature is extra data appended to a transaction that can only be created by

3. In general, maintaining complete privacy while doing online transactions is very difficult, with or without Bitcoin. Although the use of Bitcoin helps protect privacy when compared to using a credit card, it is not a complete solution. Other tools and precautions might need to be used as well (for example, using the online privacy-protecting TOR browser).

4. Although every private key is associated with a single Bitcoin address, the reverse is not always true. A Bitcoin address can require multiple private keys to unlock the bitcoins at that address (in this case, the Bitcoin address will begin with the number 3 instead of the usual 1). However, this advanced feature isn't used for most common transactions.

someone possessing the corresponding private key. Similar to a PIN, a private key should be kept secret. If someone obtains your private key, he will be able to spend your bitcoins.

Note that although a private key can be used to produce a digital signature, a digital signature cannot be used to obtain a private key. Digital signatures also cannot be reused to make new transactions; therefore, broadcasting a signed transaction to the Bitcoin network is not a risk. This action is fundamentally different from making an online payment with a credit card. When you use a credit card, you provide your credit card number to someone to authorize a transaction. That number can then be reused (maliciously) to authorize more transactions that you never intended.

Unlike a PIN, which both you and the bank know, *only you know the private key*. The risk you take in this circumstance is if you lose the private key to an address in which you've stored bitcoins, those bitcoins will remain locked in that address forever. Clearly, it is extremely important not to lose your private key! Fortunately, you can easily make digital backups of your private keys or write them on a piece of paper and keep them in a safe place. Losing your Bitcoin address is not a problem, however, as it can be recovered from the corresponding private key (Bitcoin wallet programs, described later in this chapter, can do this for you automatically).

Although it's possible to use Bitcoin with only a single address and private key, in practice most people use many addresses, each with its own private key, and store them in a digital wallet.

The Bitcoin Wallet

A *Bitcoin wallet* is a collection of addresses and private keys owned by one person. Having multiple Bitcoin addresses can help you organize your money. You may want separate addresses for paying rent, for shopping online, and for saving bitcoins to pay for a house in the future. So a person could have two bitcoins in his wallet that are distributed among many different Bitcoin addresses (see Figure 2-2).

Using multiple addresses, in the form of a wallet, also helps you maintain privacy. This is because the public ledger maintained by Bitcoin, which anyone can look at, has no way of knowing that any two addresses are in the same wallet and are owned by the same person (as long as that person hasn't done anything to show that the two addresses are linked, such as making a single purchase using bitcoins from both accounts).

To manage several addresses and private keys, people use Bitcoin *wallet programs*.[5] Whereas a Bitcoin wallet is an abstract concept, referring to a group of Bitcoin addresses, a wallet program is a concrete tool that helps users with common Bitcoin tasks, such as creating new Bitcoin addresses, sending bitcoins to others, backing up private keys, and many others. But be aware that the terminology surrounding Bitcoin wallets is not always

5. Also called *Bitcoin wallet clients*.

used consistently. Often, Bitcoin wallet programs are called *Bitcoin wallets* for short, confusing these two distinct concepts. When you save a Bitcoin wallet (perhaps to make a backup copy), you create a *wallet file*, which contains information for multiple Bitcoin addresses. Later, you can load your wallet files into a Bitcoin wallet program.

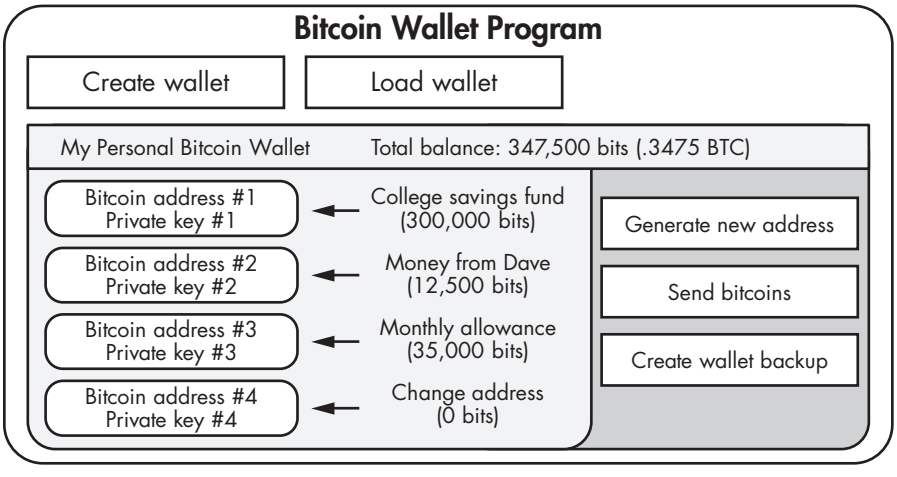


Figure 2-2: A Bitcoin wallet is an organized collection of addresses and their corresponding private keys. Bitcoin wallet programs exist to help perform common tasks like sending bitcoins and managing the bitcoins in your wallet.

Many Bitcoin wallet programs are available to choose from; most are free downloads and can be run on your laptop or phone, or even in your web browser. We'll explore the various Bitcoin wallet programs in Chapter 3, but in this chapter we'll use the Electrum wallet, which is open source, cross platform, and very simple to use.

GETTING SOME "STARTER MONEY" TO LEARN ABOUT BITCOIN

You'll need a small amount of Bitcoin (less than $1 USD) to work through this chapter. If you have a friend who's a bitcoiner, consider asking her to give you a little change to use for practice. Otherwise, go to *http://newbiecoins.com/*, which is a site we (the authors) will maintain as a public service and which will list other sites that are giving away small amounts of free Bitcoin. There are usually *some* reputable sites giving out coins for newbies, but the situation for such giveaways is fluid, with sites going up or down daily, so we can't cover specific ones in this book.

Creating Your First Bitcoin Wallet with Electrum

To follow along in this section, download and install Electrum (*http://electrum.org/*). If you choose to use a different Bitcoin wallet program, most of the instructions on the following pages should apply to it as well.

When you run Electrum the first time, you'll be asked to create a new wallet (or restore an old wallet, which we'll ignore for now), as shown in Figure 2-3.

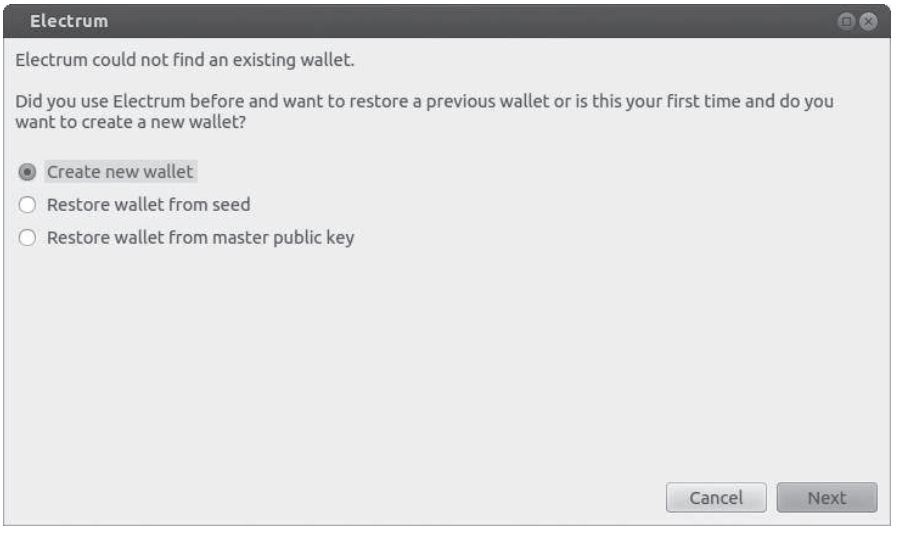


Figure 2-3: Creating a new Bitcoin wallet with Electrum

The next step is specific to Electrum; that is, it is not a standard feature of most Bitcoin wallet programs. The application presents you with a *seed*, which consists of 12 randomly chosen words, and asks you to write them down (see Figure 2-4). Electrum uses this seed to create your Bitcoin addresses and private keys; therefore, the seed must be kept secret, similar to your private keys. Because we'll be dealing with only small amounts of bitcoins in this chapter, you don't need to be too careful just yet. However, you should start keeping these security details in mind. A major benefit of a seed is that if you lose your computer (say, in a fire or theft), everything—your wallet, your Bitcoin address, your private keys, and (most importantly) your money—can be recovered from the seed.

The next step gives you the option of creating a password. Although the password is optional, it is very important. If your computer is stolen or somehow falls into the wrong hands, the password prevents others from spending your bitcoins. Because Electrum (and other Bitcoin wallet programs) uses the password to store your Bitcoin wallet on your computer in an encrypted form, the wallet is useless without the password. With many other Bitcoin wallet programs if you forget your password, you could permanently lose access to your wallet. But with Electrum, you can restore the wallet from your seed (without needing the password).

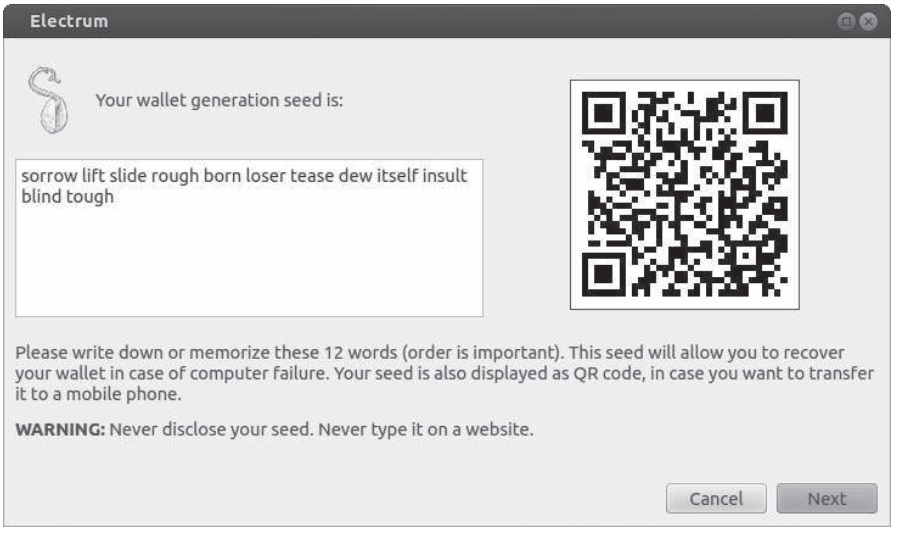


Figure 2-4: Electrum presents you with a seed.

In the final step, Electrum requests instructions on how to connect to a remote server. Select **Auto connect** and then click **Next** (see Figure 2-5).

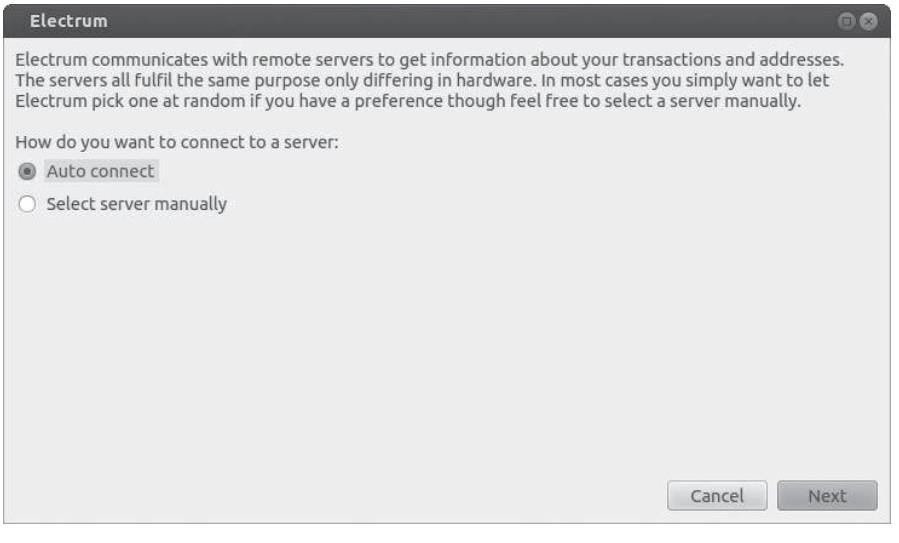


Figure 2-5: Selecting your server connection

You should see a screen similar to the one in Figure 2-6. The green dot in the bottom-right corner indicates that you are connected to the Bitcoin network. Congratulations! You've just set up your first Bitcoin wallet! Now you can fill the wallet with bitcoins.

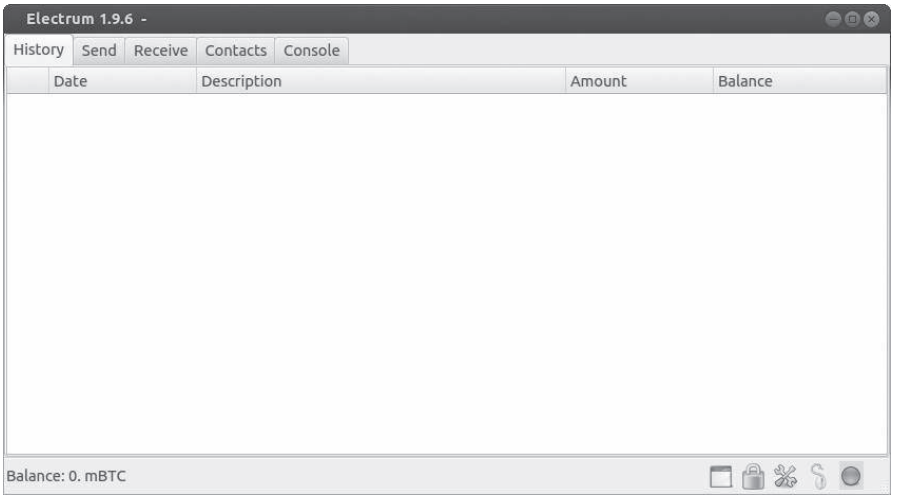


Figure 2-6: Here is your first Bitcoin wallet!

Acquiring Bitcoins in Your Wallet

On the Receive tab (see Figure 2-7), you should see a list of several Bitcoin-receiving addresses.

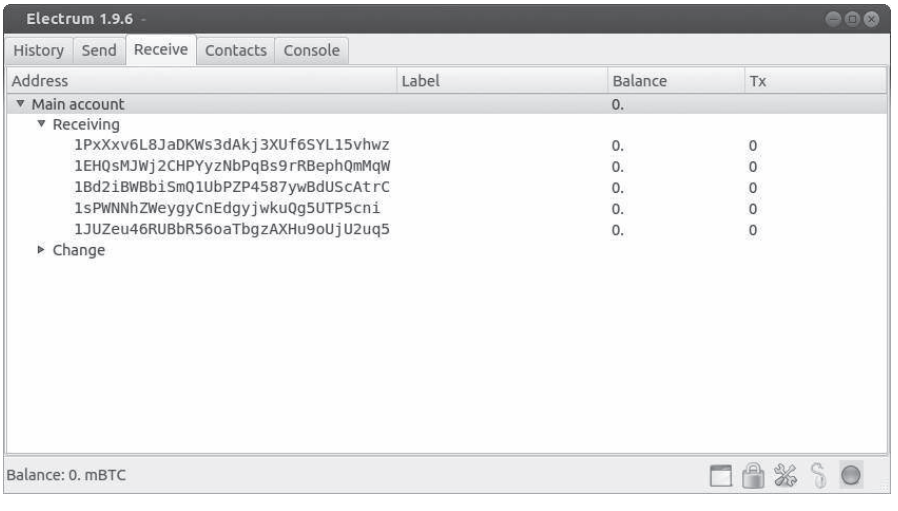


Figure 2-7: The Receive tab

You can share these addresses with your friends so they can send you some starting bitcoins—one way to acquire bitcoins! At this point, if you want to put significant money into bitcoins, refer to Chapter 4 where we discuss how to do this in detail (but be sure to first read Chapter 3, for security reasons).

To get a small quantity of bitcoins into your wallet—whether from a friend or from a site listed on *http://newbiecoins.com/*—you'll have to give that friend or website one of your public Bitcoin addresses. At the time of this writing, a small amount of Bitcoin for testing would be about 0.5 millibitcoin (mBTC). If at the time you are reading, 0.5 mBTC is a lot of money, then feel free to use a smaller amount. A few minutes after your friend (or the site) sends these coins, you should see a balance of 0.5 mBTC in your Electrum wallet. (Actually, your balance will usually update instantaneously.) Well done! You now own bitcoins, which enables you to look into your future! How? Read on.

NOTE *Importing private Bitcoin keys into a wallet can be hazardous. You should only import money using private keys when small sums of money are involved, and never use this method as part of a strategy for managing larger sums of money unless you're an advanced bitcoiner. The comic at the end of this chapter illustrates why working with raw private Bitcoin keys can be very dangerous.*

Spending Bitcoins with Your Wallet

Although thousands of merchants now accept bitcoins, you can't buy much with 0.5 mBTC. You'll need to scour the Internet for good deals!

Alternatively, for the deal of the century, you can have your fortune read online for the low, low price of 0.1 mBTC.

Visit *http://befuddled.org/* to access our fortune-telling website, which we've linked directly to a crystal ball. When you send 0.1 mBTC to the server's Bitcoin address, the server transmits a *fortune request* to the crystal ball, and it predicts your future.

To get your fortune, use Electrum's Send function and paste the website's Bitcoin address into the *Pay to* field. In the *Amount* field, specify **0.1 mBTC** (if your units are set to BTC, enter 0.0001; change the default units by choosing Tools ▸Preferences ▸Base Unit). Bitcoin transactions also require a fee. In the *Fee* field, enter **0.1 mBTC** as well (this amount may be more than is necessary, but let's not worry about that for now). Your screen should look something like Figure 2-8.

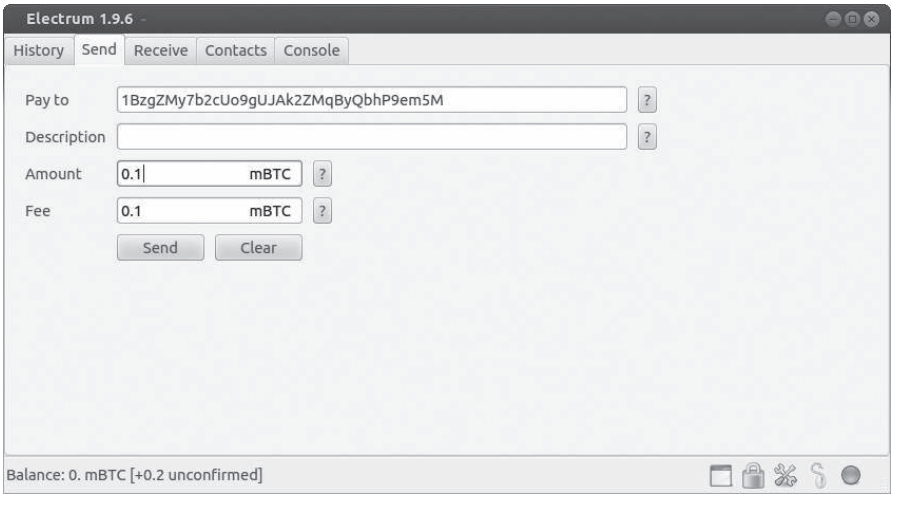


Figure 2-8: Sending bitcoins through Electrum

When you click **Send**, Electrum asks for your password and then confirms that the transaction has been transmitted. Almost immediately, you should see your fortune on the website. Welcome to the future! You've just made your first Bitcoin transaction!

Electrum's History section shows you the transactions you've made in the past. Transactions that display the word *pending* are not yet recorded on the Bitcoin public ledger (which typically occurs about 10 minutes after a transaction is sent).

If you're not interested in your fortune but want to practice sending bitcoins, you'll be pleased to know that many charities and nonprofit organizations now accept bitcoins. Some provide food for the homeless, defend online privacy rights, and support open source software (including Bitcoin). By searching online, you'll find numerous nonprofit organizations that have posted a Bitcoin address. We recommend giving your free millibitcoins to Sean's Outpost, a charity that feeds the homeless in Pensacola, Florida (its donation Bitcoin address can be found on its website, *http://seansoutpost.com/*). Unlike with the fortune-telling website, you might not

receive a response from the website when you donate. But rest assured that the recipients have accepted your bitcoins if Electrum's History section displays the word *confirmed*. (Sometimes the confirmation status is indicated by a small dial icon or more than one confirmation is given for the transaction.)

You might be wondering how and where Electrum got a Bitcoin address. The answer is your Bitcoin wallet program.

Bitcoin Addresses Generated by Your Bitcoin Wallet Program

When you run a Bitcoin wallet program, it can generate a new Bitcoin address for you offline. No communication with the Bitcoin network is necessary, an unusual feature that surprises many people. With other addresses or numbers, for example, when you create a new email address, you must first find out whether the address is being used by someone else. The same is true when get a new phone number or when you open an account at a bank. However, when you want a new Bitcoin address, one is chosen at random from all of the possible Bitcoin addresses. What are the odds that a Bitcoin address randomly generated for you will be the same as one generated by someone else? We'll use an analogy: Consider all the grains of sand on Earth—from all the beaches and deserts. When you choose a single grain at random to be yours and another person chooses a grain of sand at random to be his, the odds that both of you would choose the same grain of sand would be over a trillion times more likely than the odds that you both generate the same Bitcoin address.[6]

While you can create Bitcoin addresses offline, you must be online to see how much money is in your addresses or to send money to others. That's because these additional actions require you to access the public ledger of Bitcoin, which we'll discuss next.

The Blockchain

All Bitcoin transactions are recorded into the *blockchain*. Throughout the remainder of this book, we'll refer to the Bitcoin ledger as the blockchain. The reason for its name is that new transactions are appended to the ledger in large chunks, or *blocks*. Whenever a new Bitcoin transaction is broadcast to the network, computers on the network add it to a growing pool of other new transactions. Then, about every 10 minutes, the transactions in that pool are bundled into a block and added to the blockchain (see Figure 2-9). To function properly, all Bitcoin wallet programs need access to an up-to-date copy of the blockchain, and every time a block is added, the wallet programs copy and add the block to their own blockchain.

6. Odds of a trillion times more likely are still a dramatic understatement. The possible value of Bitcoin addresses is 2^{160} ($\sim 10^{48}$), and the number of grains of sand on Earth is approximately 10^{19}.

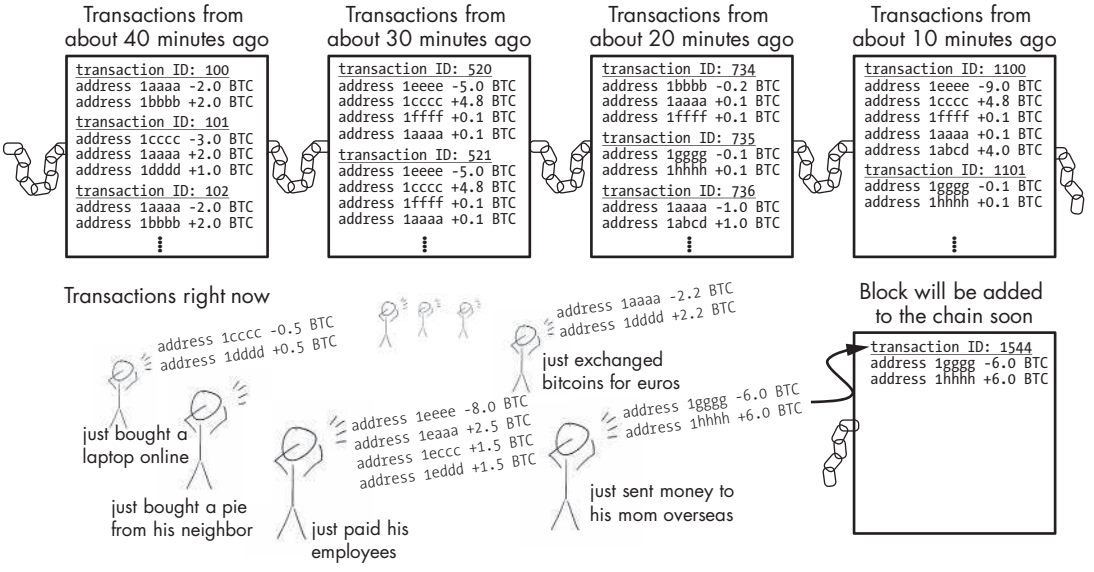


Figure 2-9: Bitcoin transactions are grouped into blocks that are added to the blockchain every 10 minutes.

The thousands of computers on the Bitcoin network that collect transactions and add them to the blockchain are called *miners*. We'll explain miners and the details of what they do later in the chapter. For now, keep in mind that anyone can be a miner (including you) by running open source Bitcoin-mining software on a computer that is connected to the Bitcoin network. At any given moment, tens of thousands of miners are connected to the Bitcoin network. All volunteer their computers for the purpose of adding new transactions to the blockchain (we'll explain why they do this in a moment).

Every block added to the blockchain is added by a *single* miner on the network. Then everyone else on the Bitcoin network follows suit and updates their own copy of the blockchain (this includes other miners and Bitcoin wallet programs). Why does only one miner add a block, and how is it decided which of the thousands of miners it is? This is where Bitcoin gets interesting—and a little technical.

Let's first consider why anyone would want to update the blockchain. Certainly, if you wanted to complete transactions, your Bitcoin wallet program would need the latest copy of the blockchain. However, you might not want to send or receive bitcoins for months, so why bother updating your copy of the blockchain in the meantime? For the Bitcoin system to work, many people need to keep up-to-date copies of the blockchain. The reason is that if only one person had the latest copy, she could manipulate the number of bitcoins people had on record. Therefore, good will alone isn't sufficient to keep the system running. But the lure of a reward is always an attraction.

The Blockchain Lottery

As an incentive for users to update the blockchain as frequently as possible, Bitcoin uses a lottery-based reward system. Many people become miners and try to be the *first* to add a block to the blockchain. Then, based on some probability, a winner is chosen and gets to add a block.

What is the purpose of using a lottery like this to run Bitcoin? Well, let's imagine Crowley wants to buy a $10,000 car from Clarice. (You'll learn more about our friend Crowley the Crocodile in the comic in Chapter 5.) Using traditional currency, two people engaging in this transaction would probably go to a bank and have the money transferred between their bank accounts (or use a cashier's check, which is analogous to this; see Figure 2-10).

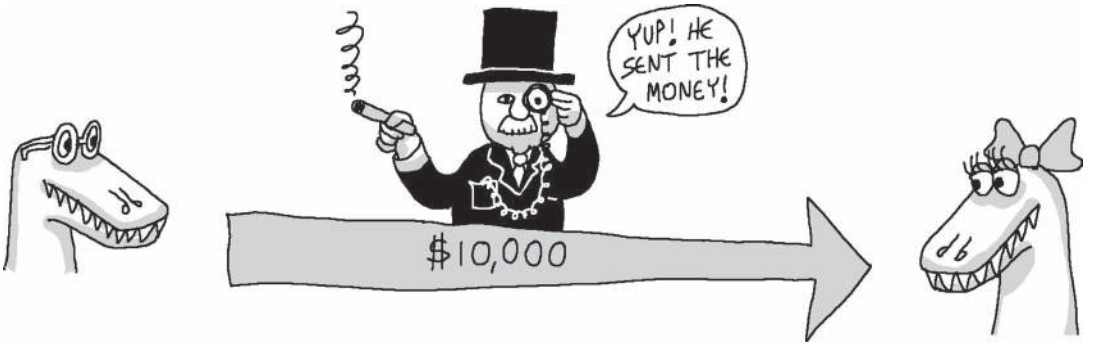


Figure 2-10: Crowley sending $10,000 to Clarice through a traditional bank

They would do this at a bank because they need a trusted third party (a "banker") that manages a "money ledger" and moves the money on the ledger from one person's account to another. The banker's job is to make an announcement that Crowley and Clarice can trust; that is, to affirm that the ledger has been updated correctly. (The banker may or may not be sporting a monocle, wearing a top hat, and smoking a cigar.)

With Bitcoin, we also need a person to adjust a ledger, which in this case means adjusting the blockchain by adding a block to it. It turns out anyone can fill this role, as long as he is not connected with either party in the transaction, because that could lead to a conflict of interest. Picking a person randomly through a lottery helps accomplish this. So with Bitcoin, a lottery picks a random miner, who then announces to the network that certain Bitcoin transactions are valid (see Figure 2-11).

Of course, there's always a small chance this miner *does* know one of the persons involved in a recent transaction. This is why blocks are arranged in a chain: In roughly 10 minutes, when the next lottery winner is announced, this winner also confirms, as part of her announcement, that she agrees with all the transactions of the previous lottery winner (see Figure 2-12).

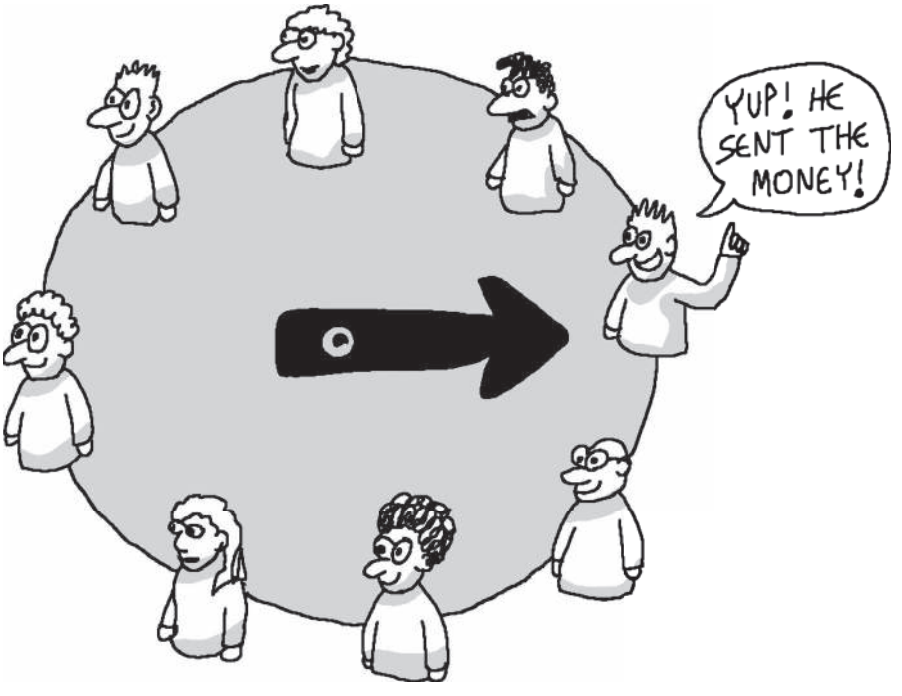


Figure 2-11: A random person running Bitcoin-mining software is chosen to confirm Bitcoin transactions.

In the process, each winner in the Bitcoin-mining lottery receives a reward, which is a certain amount of bitcoins. The reward includes all of the transaction fees for the transactions in that block, which motivates miners to collect as many transactions into a block as possible, increasing their reward. To be eligible for the reward from the next block, which is added 10 minutes later, a miner needs to have the latest copy of the blockchain to participate in the next round. This process is done automatically by open source Bitcoin-mining software that runs on computers controlled by the people involved in mining. Because of this incentive structure, thousands of miners constantly help process the transactions of Bitcoin users, making sure that the blockchain is always up-to-date.

The reward lottery is run by the community; no central authority exists to choose a winner. We'll skip the technical details for now (they're covered in Chapter 8) and just say that miners generate random numbers continuously, until they find a winning one. This takes about ten minutes. The community then verifies (also through cryptography) that the number found by the individual miner is the winner, and the miner adds a new block to the blockchain and collects the reward. When this happens, the phrase commonly used is that a miner has *found a block*.

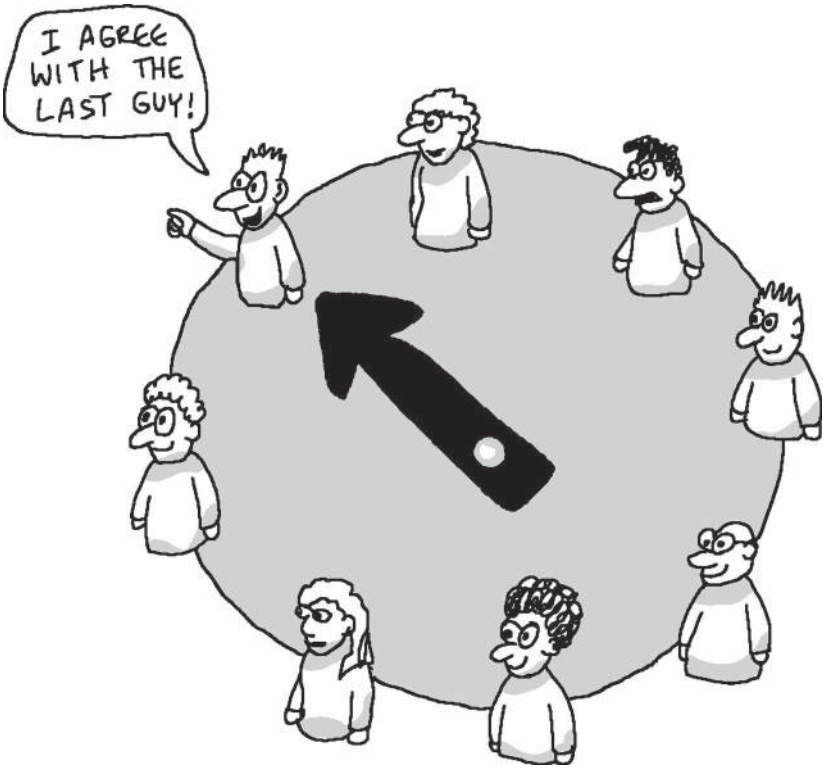


Figure 2-12: With Bitcoin, each lottery winner confirms not only her own block of transactions, but also all the preceding blocks (that she considers to be valid).

Blockchain Forking

The lottery system works as expected most of the time. But occasionally two miners find a block at the same time, and the blockchain becomes *forked*, resulting in two different branches (see Figure 2-13).

Consider the following scenario as an example: Imagine that Crowley and Satoshi are miners and find the winning number within seconds of each other. If they are located far apart on the Bitcoin network (say, on opposite sides of Earth), one part of the network will identify Crowley as the winner and another part will identify Satoshi as the winner. In this case, Crowley and Satoshi will each add a block to the blockchain (each thinking that he is the winning miner for that round). The problem occurs when one part of the network copies Crowley's block and the other copies Satoshi's. As a result, now two blockchains disagree!

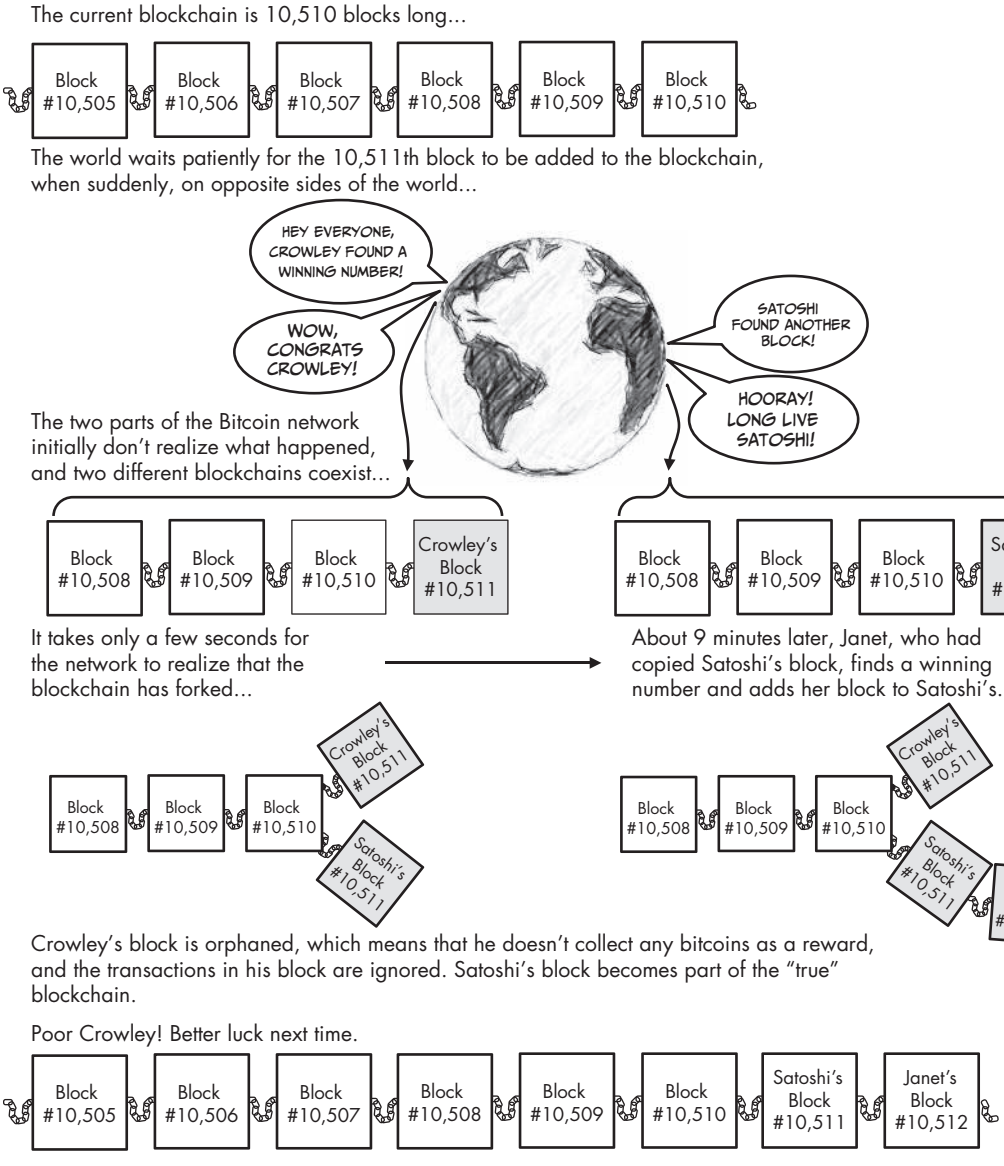


Figure 2-13: Bitcoin miners Crowley and Satoshi find a block at the same time, creating two copies of the blockchain. The resolution to the forked blockchain occurs when Satoshi's version of the blockchain adds another block before Crowley's, and Satoshi receives the reward.

Recall that your Bitcoin wallet program needs an up-to-date copy of the blockchain to function, but it doesn't know how to resolve a forked blockchain. Miners and Bitcoin wallet programs must decide which of the two versions of the blockchain to use. Forking is resolved by waiting to see which of the two branches adds yet another block first, which will happen about 10 minutes later. Then the longer branch will be considered the *true* blockchain, and the shorter branch will be ignored, or *orphaned*, by the entire Bitcoin network.

For most users, the process of forking and ignoring orphaned blocks goes completely unnoticed and has no negative impact on the use of Bitcoin. In our example, only the losing miner, Crowley, experiences a considerable impact because only one of the two miners involved can receive the reward. The losing miner is undoubtedly disappointed, but miners expect this to happen from time to time, so it comes as no surprise when it does.

Transaction Confirmations, Double Spending, and Irreversibility

A *transaction confirmation* is a common concept in Bitcoin. Some online merchants that accept bitcoins may require one or more transaction confirmations before delivering their good or service. Every transaction exists in some block on the blockchain. The blocks behind it are older, and the blocks ahead of it are newer. The position of a block relative to the tip of the blockchain is known as the *block depth*. The most recently added block has a depth of 1, the block behind it has a depth of 2, and so on. The number of confirmations a transaction has is equal to the depth of its block. So a transaction that has not been added to the blockchain (yet) has zero confirmations; it has one confirmation when it is added in a new block; it has two confirmations when a block is added ahead of it; and so on. The concept is simple enough, but why do merchants require transaction confirmations?

For low-value transactions, such as buying a cup of coffee, merchants normally forgo the transaction confirmation. You just send your bitcoins, grab your coffee, and go on your way. In general, Bitcoin transactions are irreversible, and merchants know within a few seconds after you click Send that you've paid for your drink (or whatever you're buying). However, if a merchant sells a high-priced item, such as a car, it becomes critical to consider transaction confirmations.

A malicious user with very significant computational resources (think of a James Bond–style supervillain) can try to *double spend* his bitcoins, which is essentially an attempt to trick the receiver into accepting bitcoins that were simultaneously sent to someone else as well (the "someone else" could be another Bitcoin address controlled by the supervillain). When miners on the Bitcoin network detect two transactions that spent the same bitcoins (but were sent to different addresses), they usually accept whichever one they received first and ignore the second. More important, it's impossible for both transactions to be added to a block because one contradicts the other. The supervillain's intent is for the merchant to ship the car but have the transaction be ignored and not added to the blockchain.

Fortunately, this devious scheme is usually unsuccessful because many merchants use special monitoring software and can recognize when two conflicting Bitcoin transactions are broadcast at the same time (at which point the supervillain may be kicked out of the car dealership). An even simpler solution for merchants to prevent this kind of payment fraud is to wait 10 minutes until the transaction has at least one confirmation before agreeing to ship the car. However, if a supervillain possesses truly extraordinary resources, such as many millions of dollars of computer hardware, he can attempt to make the Bitcoin network orphan the newest block in the

blockchain, resulting in a single transaction confirmation being ignored. To cope with this remote possibility, merchants who sell high-end goods typically wait until a transaction has two confirmations before handing over the keys to the buyer. In general, the higher the value of the item being transacted, the more confirmations a merchant can demand before considering the transaction to be settled. The cost for a malicious villain to double spend those bitcoins rises exponentially with each confirmation.

Now that you know the basic function and concepts of the Bitcoin blockchain, you'll learn about mining bitcoins, which is perhaps the most mysterious aspect of Bitcoin.

Mining Bitcoins

Bitcoin mining is the competitive process of collecting transactions and adding them to the blockchain in the form of blocks. Why is it called mining? The term is derived from how bitcoins are initially distributed. Although the total supply of bitcoins is capped at 21 million, this total is reached slowly over time. In the beginning, the initial supply of bitcoins was zero. Bitcoin miners receive a reward for processing other people's transactions; each reward is a small sum of *newly minted* bitcoins that increases the total supply in circulation. In this sense, Bitcoin mining is similar to gold mining: Earth has a fixed amount of gold, and miners slowly dig it out over time.

As mentioned earlier, miners must find a certain winning number by generating numbers at random repeatedly to win these newly minted bitcoins. Because fast computers can generate these random numbers more rapidly, this creates an incentive for miners to use increasingly powerful computers to mine bitcoins. In the very early stages of Bitcoin, personal computers were commonly used to generate random numbers, but soon people started building special-purpose computers designed solely for Bitcoin mining. Today, mining bitcoins requires significant capital, expertise, and access to inexpensive electricity. In fact, the evolution of Bitcoin mining resembles the way gold mining has changed over times. At one time unearthing gold could be done by a person panning in a riverbed, but now excavation is performed by large companies with expensive drills.

The mining reward for finding a block has two components: The first part is transaction fees. When you send bitcoins to someone, a small amount of additional bitcoins is added as a transaction fee.[7] Transaction fees are typically a few cents and are part of the reward that miners receive when they win the lottery and add a new block to the blockchain. Because a block is a collection of hundreds or thousands of transactions, the miner's reward is the sum of all the transaction fees in that new block. The second component of the reward is a certain number of newly minted bitcoins.

The number of newly minted bitcoins that is provided as a reward diminishes gradually over time. The first 210,000 blocks—which based

7. Strictly speaking, this transaction fee is voluntary, but miners may ignore transactions that have no attached fees.

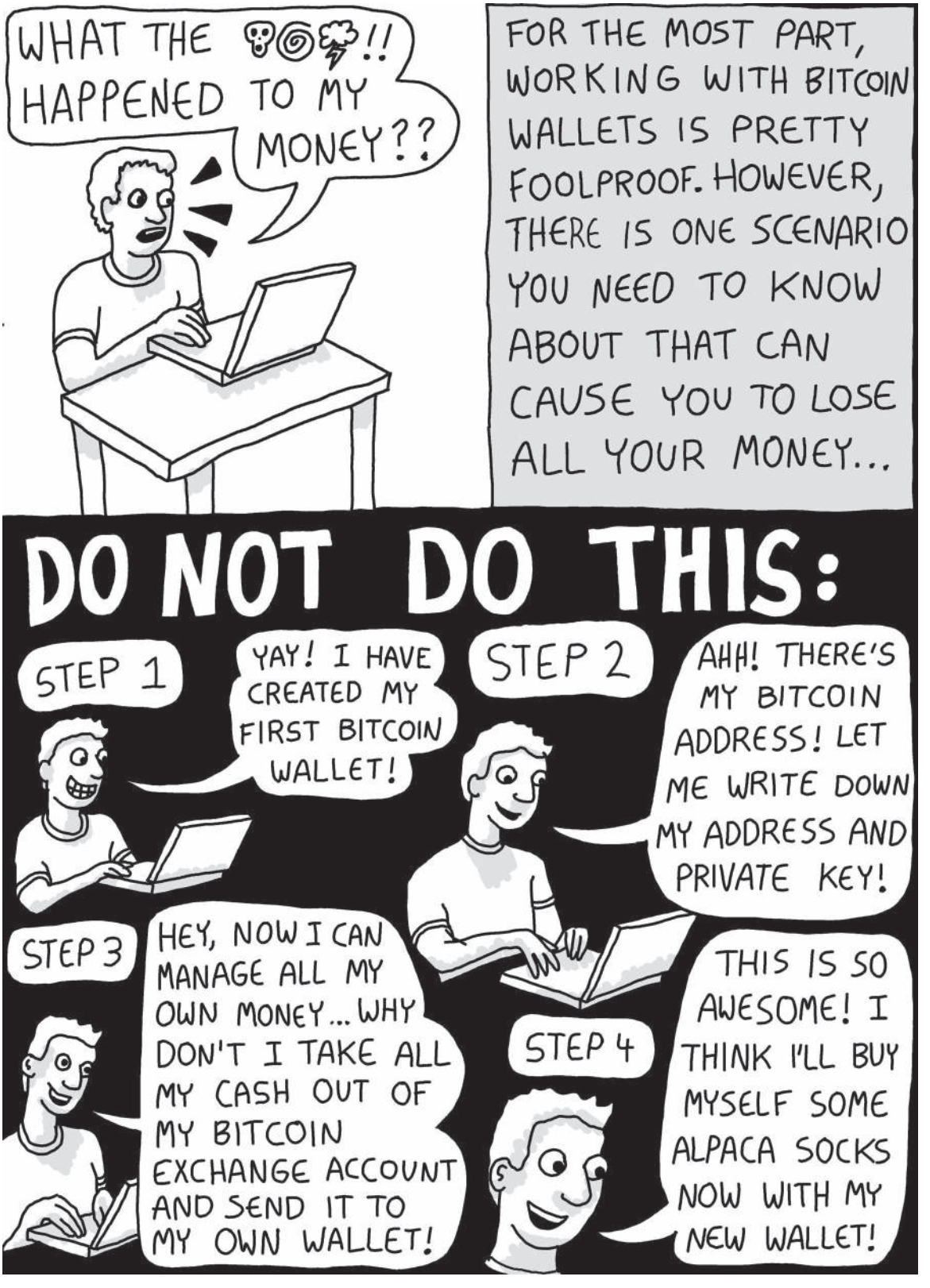
on a 10-minute spacing took about 4 years to mine—provided every winning miner with 50 newly minted bitcoins per block in addition to the transaction fees. The next 210,000 blocks (blocks (210,001 through 420,000) reward miners with only 25 newly minted bitcoins per block. Thereafter, the reward drops to 12.5, then 6.725, and so on. Because this mining process is the *only* source of new bitcoins, it is the reason no more than 21 million bitcoins will ever be in circulation.

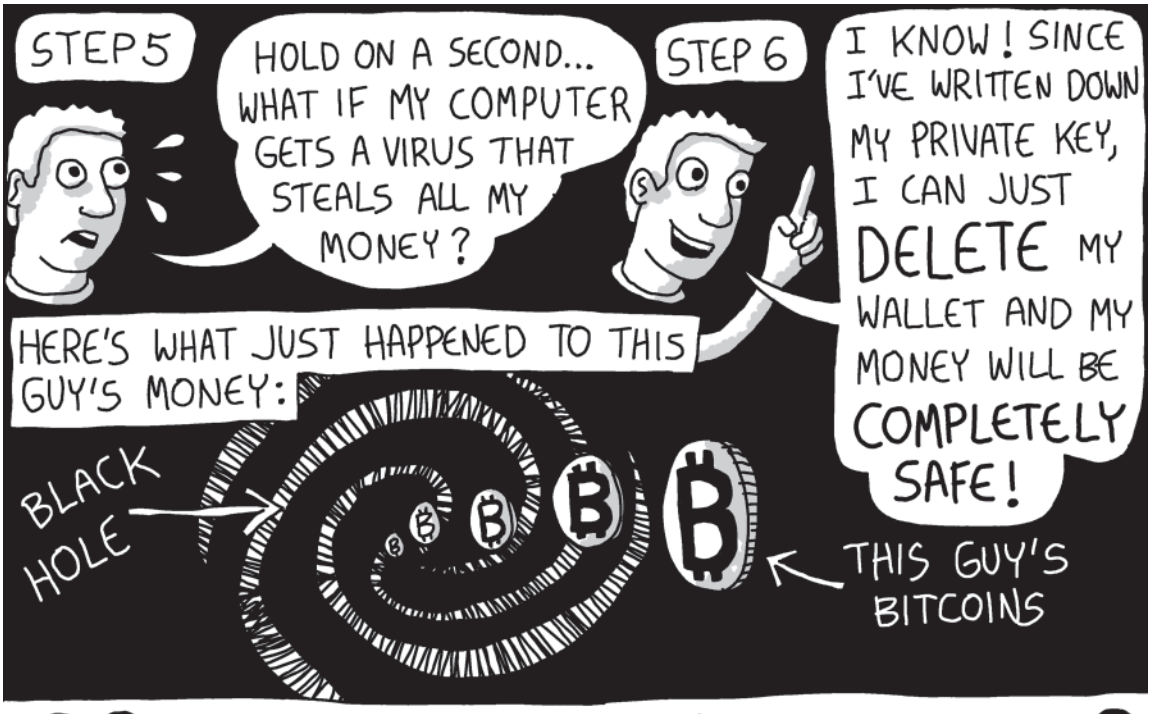
Although every four years the number of newly minted bitcoins rewarded per block halves, the transaction fees per block will continue to grow as the Bitcoin user base grows. Eventually, the user transaction fees will be greater than the reward of newly minted bitcoins. At that point, the Bitcoin network will be sustained entirely through transaction fees.

The Complexity of the Bitcoin System

Most of us are used to using centralized payment services (e.g., PayPal, credit cards). We place our trust in the companies that run those services and don't need to know how the payment system works. But Bitcoin doesn't have a company to trust; instead, we can examine the system to decide whether or not we trust it.

If you investigated the system major credit card companies use to facilitate payments, you might be surprised by how complicated it is. Because we don't normally think about how digital payment systems work, it is not unusual that the Bitcoin system is befuddling and complicated to most. After reading this chapter, you should have a fairly good idea of how the entire system works. In later chapters, we'll delve further into certain details, such as the specific hardware and programs that Bitcoin miners use; however, the overall explanation of the Bitcoin system will not change from how it is described in this chapter. From this point on, we can focus on acquiring bitcoins and thinking about how they'll impact our global economy!

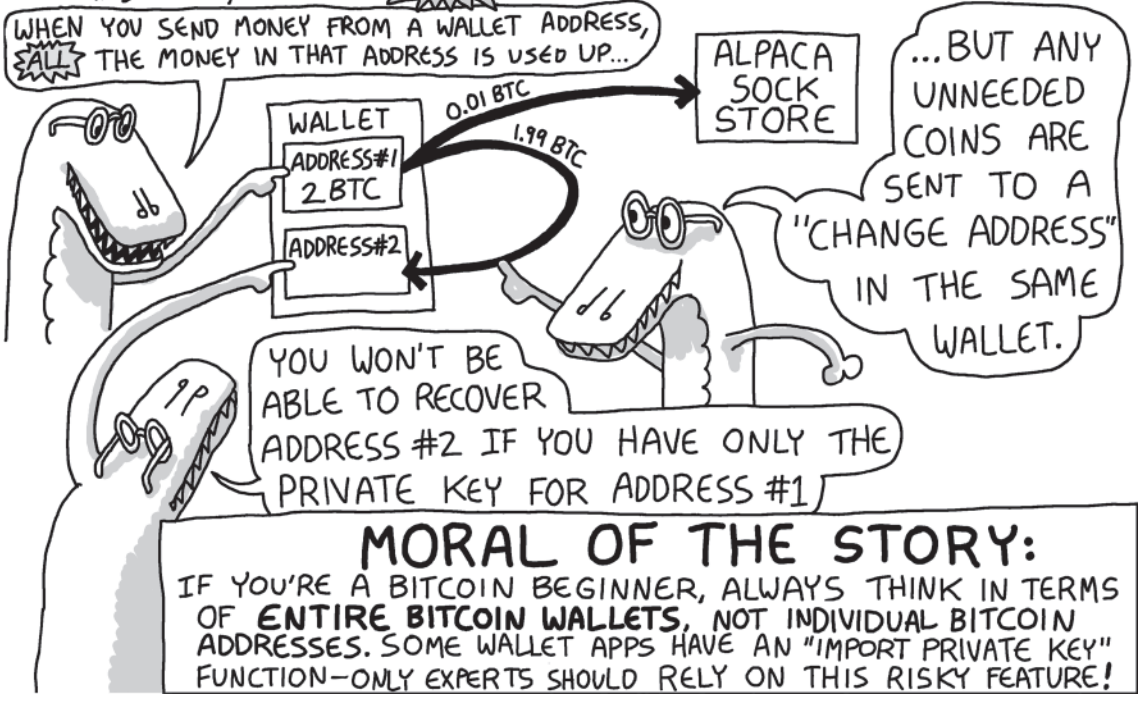




SO WHAT WENT WRONG?

A BITCOIN WALLET IS NOT JUST A BITCOIN ADDRESS.

INSTEAD, IT'S A LIST OF BITCOIN ADDRESSES.



MORAL OF THE STORY:

IF YOU'RE A BITCOIN BEGINNER, ALWAYS THINK IN TERMS OF **ENTIRE BITCOIN WALLETS**, NOT INDIVIDUAL BITCOIN ADDRESSES. SOME WALLET APPS HAVE AN "IMPORT PRIVATE KEY" FUNCTION—ONLY EXPERTS SHOULD RELY ON THIS RISKY FEATURE!