IN THIS CHAPTER

- Discovering the history of digital currency
- Finding out about early Bitcoin and its creator
- Understanding what money (and Bitcoin) is and is not
- Exploring the benefits of Bitcoin

Chapter 1
Bitcoin in a Nutshell

For a mere teenager, the Bitcoin network has certainly had a big impact on the world, transacting more than US$12.4T in 2021 alone. As we write these words, Bitcoin has a *market capitalization* (total value) of $918,705,395,133, which is almost a trillion dollars. (The market cap is the total number of Bitcoins in "circulation" multiplied by the current market price of a single Bitcoin.)

But that's a current low price; just a few weeks prior, it had a combined value of almost 1.3 trillion dollars. By the time you read this, the value may be higher, lower, or the same. That's one of the things about Bitcoin: Its market price can be very volatile, as you'll soon learn if you spend a little time watching the markets.

But the impact we're talking about is not just referring to Bitcoin's current market value. In fact, the market cap of Apple, Inc. is more than three times that of the Bitcoin network. However, a comparison with Apple might be apropos right now.

Figure 1-1 shows how much Bitcoin would be needed to buy a single share of Apple stock, from 2010 through 2021. The value of a single Bitcoin has been increasing against the Apple stock (just as it has, of course, against the U.S. dollar and other governmental currencies).

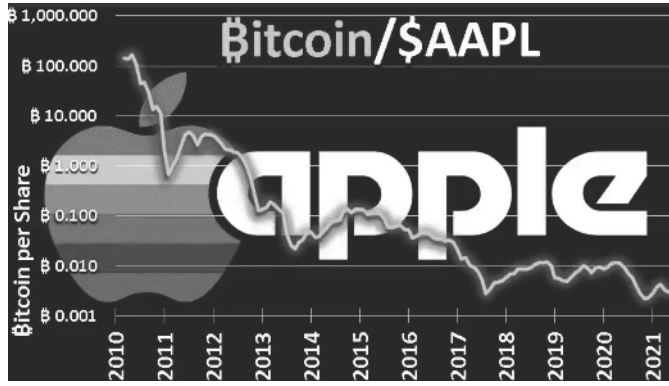

FIGURE 1-1: How much Bitcoin is needed to buy a share of Apple?

The launch of Bitcoin set off a revolution in blockchain and cryptocurrency. There are now more than 13,000 different cryptocurrencies. (Most, be warned, are essentially valueless and will remain that way.) At the time of writing, the top five cryptocurrencies have a combined market cap of almost 1.7 trillion dollars, and a number of cryptocurrencies have genuinely useful functions beyond merely being used as money or a store of value. It's likely that some of these cryptocurrencies will endure, even if most won't.

But we're here to talk about Bitcoin, so let's begin with a little history. Where did Bitcoin come from, and how did it develop?

In the Beginning, There Were . . . Digital Currencies?

Blockchain-based cryptocurrencies are pretty new, but digital currencies designed for use online have been around for quite a while. (Don't worry about this *blockchain* thing for the moment;

we explain that in not-too-mind-numbing detail in Chapter 2. Just understand for now that a blockchain is a special kind of database, a store of digital data.)

As people started flooding online — the process began in the early 1980s, but really took off in 1994 with the advent of the commercial Internet — it became clear that they were going to need some way to spend money in cyberspace (the first Internet stores opened in that year). Of course, most online transactions today use credit and debit cards — even PayPal and Venmo are essentially enabling such transactions, along with bank transfers — but that wasn't the case in the early days. Many people were concerned about credit-card theft and thus wary of using their numbers online, for instance. (When co-author Peter opened an online store in 1997, he did have a functioning credit-card gateway, but many customers would print out a paper order form and mail a check!)

There was also the issue of *microtransactions*. Surely, in the digital world, it should be possible to pay someone, say, five or ten cents for something, such as access to a video or article. The microtransaction problem has still not been solved (though one might argue that the Bitcoin Lightning network, which we discuss in Chapter 4, almost gets us there), but nonetheless, that's one of the ideas that drove the development of digital currencies.

And develop they did. In 1983 David Chaum wrote a research paper on the concept of digital currency (*Blind Signatures for Untraceable Payments*), suggesting the use of cryptography to create and manage a digital currency. So even back then, cryptography had a role in digital currencies, although they weren't known as cryptocurrencies back then. When you hear people talk about cryptocurrencies, they are generally talking about this new generation of blockchain-based cryptocurrencies that started with Bitcoin. (We explain more about cryptography and how it relates to cryptocurrencies in Chapter 2.)

Chaum actually launched a cryptography-based digital currency, known as *DigiCash*, in 1990, but these were still very early days. Very few people were online in 1990, and the currency died out by around 1998. What likely hurt digital currencies by the end of the '90s was that the credit-card companies wanted a

piece of the online action, and thus went out of their way to assuage consumers' fears of using credit cards online.

Still other digital currencies came along. There was e-gold, a currency backed by real gold, and Millicent, a currency created by a major computing company, Digital Equipment Corporation (DEC). (If you're younger than, say, mid-thirties, you probably won't remember DEC, but it was a big deal. In fact, even IBM had a micropayments division working on digital currencies at the time.)

Then there was NetBill, a project of Carnegie Mellon University, which was later merged into another system, CyberCash, which eventually ended up in the clutches of PayPal. There was Beenz, which had a partnership with MasterCard at one point, First Virtual, CyberCoin, Flooz (promoted by Whoopi Goldberg, no less!), and various others.

But nothing much *stuck*. Lots of great ideas, but nobody could quite make it all *work*. By the early 2000s, most of these endeavors were moribund (probably ushered along by the dotcom crash of late 2000). There were exceptions. Liberty Reserve, based in Costa Rica, ran from 2006 until 2013, but was shut down after accusations that it was being used to launder billions of dollars of criminal proceeds. And closed systems that work on particular networks, such as China's QQ Coins, are mostly used on the Tencent QQ Messaging service.

But then, there was Satoshi Nakamoto and his magical blockchain.

The Birth of Bitcoin

On November 1, 2008, someone named Satoshi Nakamoto posted a message to a cryptography forum, titled *Bitcoin P2P e-cash paper* (archived at `https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html`). In his message, Nakamoto announced that he had "been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party."

In other words, he'd created a currency system that worked on a network of peers — computers working together with each equal to the other. With no central power required, no bank or government to act as a "trusted third party" was required.

A comment he made in the post explained his view of the problem with the earlier cryptocurrencies. "A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s," he said. He believed that these other digital-money systems had a critical weakness, an Achilles heel. "I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."

TECHNICAL STUFF

Nakamoto had previously set up a domain name and a simple website, bitcoin.org, and there he posted a document explaining how all this would work: `https://bitcoin.org/bitcoin.pdf`. You might want to take a quick look, though it's not essential for your understanding of Bitcoin (it's pretty geeky stuff).

The whitepaper he posted describes how a *blockchain* (a special form of database) could be used to manage the currency. Essentially, the blockchain records a ledger, a record of currency transactions, and because the blockchain is duplicated over numerous computers (the *peers)* and because these peers are all equal, no trust in a central party is required. You may hear Bitcoin described as a "trustless" system. That doesn't mean it can't be trusted; it means that a trusted third party is not required. The trust, in effect, is baked into the system. The mathematics — or mathemagics, as Peter likes to call it — which powers the system means that Bitcoin transactions *can* be trusted, even without a central "power" overseeing the system. (See Chapter 2 for an explanation of why.)

REMEMBER

Satoshi Nakamoto (whoever he, she, or it is) didn't use the words *cryptocurrency, blockchain,* or *trustless* anywhere in the whitepaper. Those are terms that others applied to the system later.

The idea of blockchain had actually been around for a while — at least since 1991 — in fact, remember David Chaum of DigiCash fame? He had been working with the idea of a blockchain since the early 1990s.

Anyway, Nakamoto didn't stop there. In January of 2009, he/she/it launched the Bitcoin network. Nakamoto released some thirty-thousand lines of code that defined the network protocols and processes necessary to operate this peer-to-peer, decentralized money system. And Bitcoin was born.

Of course, in January of 2009, Bitcoin had essentially no value. Still, the *genesis block* created by Nakamoto (the very first block of data in the blockchain creating the first 50 Bitcoins), along with subsequent blocks of data "mined" by Nakamoto (see Chapter 7), comprise perhaps a million Bitcoins: At current prices, that's $47,369,000,000. Yes, close to 50 billion dollars!

But Who Is Nakamoto?

So who is this Satoshi Nakamoto? Nobody knows. Well, somebody must know, but either they're not saying or they've been unable to convince anybody. In fact, it's not even clear *what* Satoshi Nakamoto is. A man? A woman? A group of collaborators? An organization or firm? We don't know for sure, though most assumptions seem to be that it's a man or a group of two or three people. Perhaps not surprisingly, the most cited targets are generally cryptographers and mathematicians.

There's the actual Satoshi Nakamoto, of course — that was an obvious choice. A Japanese-American resident of California who was born Satoshi Nakamoto, and now goes by the name Dorian Prentice Satoshi Nakamoto, seems to have some of the skills needed to be *the* Nakamoto, but he denies being the founder of Bitcoin.

Then there's Nick Szabo, a digital-currency enthusiast who has been tagged as Nakamoto but denies it. Elon Musk has been "accused," too, but he denies it (and we personally think he was probably too busy to find the time!). There's Japanese mathematician Shinichi Mochizuki (he denies it), Finnish economic sociologist Dr. Vili Lehdonvirta (denies it), and Irish cryptography student Michael Clear (yep, denies it).

One of the loudest candidates is Craig Wright, an Australian computer scientist. He certainly claims he is Nakamoto, though he's accused by many of carrying out an elaborate fraud. As we

write these words, a jury found Wright liable to pay the estate of David Kleiman, a deceased friend and colleague, $100 million for misuse of funds in a joint venture they worked on. But separately, the jury also found that David Kleiman was not a partner in the creation of Bitcoin.

The jury didn't find that Craig Wright *is* Nakamoto, though — only that *if* he is, he doesn't have to share his $50 billion with Kleiman's estate. Not a bad deal. In fact, it's such a good deal that Wright stated that he was *relieved* that all he has to pay is $100 million! Still, the case is not over. Whether Kleiman's estate actually has ownership in the joint-venture company is unclear, and Wright might owe $100 million to his ex-wife. It doesn't settle the question of whether or not Wright actually is Nakamoto. (Wright says that the jury found that he *is* Nakamoto; they didn't.) That won't be settled until Wright — or the *real Satoshi Nakamoto* — moves some of the Bitcoin out of the blockchain addresses owned by Nakamoto.

Regardless, the Bitcoin network has continued to function as designed long after Satoshi Nakamoto mysteriously stopped participating in the network, shortly after claiming Julian Assange and Wikileaks had "kicked the hornets' nest" once they began accepting Bitcoin for donations for their controversial reporting in 2010.

Understanding What Bitcoin Actually Is

So what is Bitcoin? Well, we can tell you what it isn't very quickly. It's not tangible — there's nothing you can touch or hold. You can't taste it or smell it. You can't even see it. In fact — and we explain this in more detail in Chapter 2 — Bitcoin really *isn't.* That is. . .*there is no Bitcoin.*

What there is, though, is something known as the Bitcoin *ledger* (another word, by the way, that Satoshi Nakamoto didn't use in his famous Bitcoin whitepaper, but that is what the data stored in the Bitcoin blockchain has come to be popularly known as). A ledger is a written record of transactions; your checkbook's little

account register is a form of ledger, for instance. (For those of you under 30, a check is a piece of paper you can write a number on, sign your name, and give to someone, and that someone can then give it to their bank and the bank gives them money. . .an amazingly efficient system.) Or consider a bank statement, showing money coming into and leaving your account. (All too often *leaving*.) That's a form of ledger, too.

So, when Satoshi Nakamoto created the first ever Bitcoin, how did he create it? Well, when we talk about Bitcoin being "created," we're really talking in shorthand. No Bitcoin *thing* was created. When Nakamoto first "created" Bitcoin, what he really did was to create a set of rules for a ledger in which he *recorded* the creation of Bitcoin. The ledger says, in effect, "50 new Bitcoin were created today." And there you go, Bitcoin exists.

When Nakamoto minted that first "genesis block," the nature of the network was set in computational stone. Buried in the first block of data was a little additional text, words from the front page of that day's *New York Times* (January 3, 2009): "Chancellor on Brink of Second Bailout for Banks." Perhaps this was a hint at Nakamoto's reason for creating the network, as an alternative to what he felt were the corrupt government-managed monetary systems.

The ledger essentially records two things. The first is the *creation* of Bitcoin, which is done through a process called "mining." Nakamoto "mined" those original 50 Bitcoins (however, the first 50 Bitcoins are unspendable due to the nature of the code). Mining continues, and in fact, new Bitcoins are created each time a new block of transactions is added to the Bitcoin blockchain, every ten minutes or so. (Chapter 7 explains how this "mining" process works.)

However, there is a mathematical arrangement to all this: Bitcoins are created on a steady schedule, and every four years or so (during an event quaintly called *the halvening*), the number of Bitcoins created every ten minutes is halved. Right now, 6.25 Bitcoins are created every ten minutes, but sometime in 2024, that will be reduced to 3.125, then again halved four years later, and so on (every four years) until around the year 2140, when the maximum number of Bitcoins will finally be in circulation.

The second thing that the ledger records is what happens to the Bitcoin once it has been created. As we discuss in Chapter 2, all

Bitcoin is associated with "addresses" in the blockchain, and as people buy and sell Bitcoin, or use Bitcoin to buy something (essentially the same as selling Bitcoin), the coins get sent from one address in the blockchain to another. The Bitcoin ledger keeps track of where the Bitcoin flows, from address to address to address. Each address is under the control of someone, and thus the blockchain is, in effect, keeping track of who owns what. If the Bitcoin blockchain ledger says the address you control has 2 Bitcoins associated with it, then you control those 2 Bitcoins. (In Chapters 3 and 4, we explain how to exercise this control — that is, how you can transfer your Bitcoin to other addresses in return for governmental fiat currency or for goods and services.)

FIAT CURRENCY?

Hang around in the Bitcoin community long enough and eventually, you'll hear people talking about *fiat* currency, usually disparagingly. A fiat currency is currency by decree, by official order. A fiat currency is one that is issued by a government, without being backed by a commodity such as gold. (To quote Nobel-prize winning economist Paul Krugman, "fiat currencies have underlying value because men with guns say they do.") Most currencies these days are fiat currencies; the "gold standard" generally fell out of favor in the 1930s, during the Great Depression. (Great Britain dropped the gold standard in 1931.) The U.S. dollar used to be pegged to silver, but in 1900, a law was passed linking it to gold. It remained linked to gold through most of the century, until being completely de-linked from gold in 1971 and becoming a fiat currency. (However, in 1934 the U.S. did devalue the dollar against gold; that is, they reduced the weight of gold per dollar.)

The advantage of fiat currency is that it gives governments more control over the money supply. Many economists, probably most, believe that adherence to the gold standard prolonged the Great Depression, as governments were not able to stimulate their economies by increasing the money supply. The disadvantage, according to many true believers in Bitcoin, is that it provides governments with too much control over the money supply!

Now, if this all sounds a little flakey, a bit like a con game — and there are certainly plenty of people who will tell you that Bitcoin *is* a con game — we're going to explain in a few moments what *money* is. You may think you know what it is, but you probably don't, and without understanding what money is, it's hard to understand how Bitcoin *can be* money. But first, a little more about Bitcoin.

Understanding Bitcoin Units

To begin with, you need to understand that Bitcoin can be broken down and bought and sold in pieces. A Bitcoin is not like a gold coin; if you buy, for instance, a US$10 Liberty Gold Coin (for around $1,000, by the way), you're buying the whole thing. You're not buying half or a quarter.

But with Bitcoin, which can sell at $50,000, $60,000, or whatever *per coin*, most people can't afford to buy in if they have to buy the entire thing. And in any case, there is no *coin*. It's just an entry in the ledger.

So that entry in the ledger can say whatever we want it to say. It can say that you bought half a Bitcoin, or a tenth or hundredth, or a ten thousandth, all the way to a single one hundred millionth. That is, you can buy partial coins — fragments of a Bitcoin. Table 1-1 offers a quick look at Bitcoin units.

TABLE 1-1 Bitcoin Units

Unit	Unit Name
1; one	Bitcoin, BTC, ₿
1/10; one tenth	deci-Bitcoin, dBTC
1/1,000; one thousandth	milli-Bitcoin, millibit
1/1,000,000; one millionth	micro-Bitcoin, µBTC, bit
1/100,000,000; one hundred millionth	Satoshi, sat

The table doesn't show all the units, but these are the units you're most likely to see and hear about. Because Bitcoins are divided into Satoshis — one hundred million Satoshis in each Bitcoin — you can divide a Bitcoin into tenths: deci-Bitcoin, centi-Bitcoin, milli-Bitcoin, micro-Bitcoin, and so on. (In fact, there is even a theoretical way to divide a Bitcoin down below the Satoshi level into *milliSatoshi*, using a special ancillary network called the Lightning Network, which we talk about in Chapter 4.)

Is there enough of the smallest Bitcoin unit to go around? Well, let's take a look. There will only ever be 21 million Bitcoins; that means there will only ever be, at its maximum, 2,100,000,000,000,000 Satoshis in circulation.

Today, though, around 19 million Bitcoins are in circulation, and somewhere around 1,900,000,000,000,000 Satoshis.

With around eight billion folks living on the planet, today, about 237,500 Satoshis are in circulation per person (the number fluctuates; see the Satoshi clock at `https://satoshisperperson.com/`). Today, that's valued at around US$110.

To put this into perspective, roughly US$2,500 are in circulation ("M1" money supply) per person on the planet today (according to the Federal Reserve website at `https://fred.stlouisfed.org/series/M1SL`). That's 250,000 cents per person, similar to the number of Satoshis.

REMEMBER

All this means is that you don't need a huge sum of money to get started with Bitcoin. You can buy small pieces of a Bitcoin, but beware the fees. Buying small quantities at a traditional exchange (see Chapter 3) can be expensive; in some cases, you'll likely be paying more in fees than the price of the Bitcoin. Some exchange sites now have fee-free transactions. See, for instance, Strike (`https://strike.me/en`).

Cryptocurrency or Cryptoasset?

Bitcoin is commonly described as a cryptocurrency. Is it really a currency? We would argue that it is not. We provide more detail about this in Chapter 3, but for the moment at least, you can

think of Bitcoin as more like an asset than a currency. It's more like gold than dollar bills. It's hard to spend Bitcoin, just as it's hard to spend gold. Sure, you can do it, but it's not always simple, and most places where you'd want to spend your Bitcoin won't accept it.

And furthermore, why would you want to spend your Bitcoin when it might double or triple in value over the next few months? No, Bitcoin is not a true currency, though it was originally intended to be one (and perhaps in the future, it will become one).

Google and the Oxford Languages dictionary describe *currency* as "a system of money in general use in a particular country." Bitcoin is certainly not a currency in, say, Europe or North America. Perhaps the only country in which it comes anywhere close to being a currency is El Salvador, the government of which launched Bitcoin as a secondary currency. But for most of us, Bitcoin is a *store of value*, not something we're going to use to buy groceries.

Still, we will be talking about how you can buy and sell Bitcoin — and selling Bitcoin is, of course, essentially the same as exchanging it (you swap it in return for goods or services) — in Chapter 3.

If There Is No Bitcoin, How Can It Be Valuable?

As we write these words, anyone owning a Bitcoin can sell it for around US$48,000. But we've just told you *there is no Bitcoin. . .*that all there is, is a ledger stating that the Bitcoin exists, and who (which address in the blockchain) owns it. How can that possibly hold value!?

To understand that, we need to understand a little about money and how it works. As with *any* form of money, Bitcoin is all about *belief*. If enough people believe a form of money has value, then it has value. It can be exchanged for goods and services with other people who believe it has value. Once people stop

believing, though, the money no longer holds value. And that does happen sometimes. There have been around 60 *hyperinflation* events in human history, in which people lost faith in the currency, and it precipitously dropped in value until it was essentially worthless. Most recently, it happened in Zimbabwe; in 2008, the country actually abandoned its currency in favor of using foreign currencies. (Ironically, Zimbabwean dollar bills then rose in value, as collectors worldwide started snapping them up.)

So, again, as long as people *believe* in a particular form of money, that form of money has value. Let's say you own half of a Bitcoin; in other words, the Bitcoin blockchain *says* that you own half of a Bitcoin. (Remember, there is no actual physical Bitcoin, just a record of Bitcoin transactions.) You want to cash out, to convert that Bitcoin into your local currency. The Bitcoin blockchain says you own the address in the blockchain with which that coin is associated (we explain how that works in Chapter 2), and so you can transfer it to *someone else's* address.

Currently you can find someone who sees value in having that Bitcoin associated with their address in the blockchain. Why? Because people believe in this form of money, and so potential buyers know that when they are ready to sell it, there will be *someone else* who believes in it enough to pay for it or exchange goods and services for it. (Plus, they are hoping the money will go up in value, something we discuss more in Chapter 6.)

Belief is what makes Bitcoin work. That may sound a little woowoo or weak. You may think that's not much on which to base a form of money, but in fact, that's pretty much what *all* money is based on. Let us tell you a story.

Milton Friedman and the rai stones

Eminent, Nobel Prize–winning economist Milton Friedman wrote a paper in the 1990s about *rai stones* — a form of money once used on the Yap islands — comparing this system to the use of gold by Western nations to back their currencies.

The Yap islands are a group of four small islands in the middle of the Pacific Ocean, about 800 miles east of the Philippines. With a population of around 12,000, Yap isn't known for much, except perhaps, most notably, for an unusual form of money it used to have, known as *rai* (or *fei*) *stones.*

Rai stones were "coins" made of limestone. You couldn't carry these coins around in your pockets because they were large, sometimes very large. The stones had holes in the middle for a log to be threaded through so they could be carried! (If you'd like to see what we're talking about, do a quick image search online for rai stones.)

They mostly weren't carried, though; in fact, they sat where they were long enough to gather moss. Anyway, here's how these things worked. Let's say you wanted to buy a bunch of coconut copra (the dried kernels from which coconut oil is extracted, which is big business in the Yap islands). You would go to the seller and say something like, "You know my rai stone in the woods by the river? Well, I'll give you the rai stone in exchange for the copra." Assuming the price was right, you and the other party would then tell everybody that you no longer owned that particular rai stone, that it was now in the possession of the seller.

Note, by the way, that there was a degree of rarity to these stones. You couldn't simply grab a piece of limestone and make your own money. Apart from the amount of work required to create one of these things, there was an additional problem: There *isn't* any limestone on the Yap islands! Instead, limestone has to be quarried in Palau and brought back, a round trip of about 600 miles. (This is known in currency circles as *proof of work,* something you can learn more about in Chapter 7.)

There's even a famous story (well, famous for people who know about rai stones!) about a large rai stone falling overboard during a journey back from Palau. One can imagine the conversation.

Sailor 1: "Oh, no, we've lost that huge stone, that was valuable!"

Sailor 2: "Oh, boy, we're going to be in trouble! Oh, but wait, we know more or less where it *is,* right?"

And thus, that particular rai stone remained in circulation as long as the owner could say, "You know that rai stone I own, the one that sunk?"

Now, back to Milton Friedman. In his paper about this form of currency, he discussed what happened when the islands were occupied by Germany. (Rai stones were in use right up until the early 20th century.) The German authorities, he writes, were unable — not surprisingly — to get the local population to provide labor (to improve roads and paths on the islands, for instance).

But the German administrators had an idea. They sent someone out to paint black crosses on the rai stones, telling the locals this meant that they — the Germans — now owned them! They were, in effect, fining the local population for not providing labor.

This actually worked, which shows that the Yapese — perhaps like some readers of this book — didn't really understand what money was (a belief) and how it functioned (carried value only as long as people believed in that value). The local population provided labor to get their money back (the crosses were erased).

Now, Friedman took the story further. He discussed an event that occurred in 1932, far from the Yap islands. France asked the Federal Reserve Bank of New York to convert some of its dollar assets into gold. Rather than shipping gold to France, the bank employees simply went into its vaults and moved the gold around a little, putting the appropriate amount of gold bars into particular drawers, and marking those drawers to show they were owned by France. (This event actually led to a banking panic in the U.S., as newspapers decried the loss of gold to France.)

Friedman compared the marking of the rai stones with the marking of the gold; he explains that Federal Reserve officials set apart the amount of gold required and marked the gold to indicate that it belonged to France. As Friedman explains, "For all it matters, they could have done so by marking them 'with a cross in black paint' just as the Germans did to the stones."

You can read this paper at `https://miltonfriedman.hoover.org/internal/media/dispatcher/215061/full`. It is actually

helpful, a way to shake up your thinking about money and what it really is. Let's just see how Friedman finished up his paper:

> What both examples—and numerous additional ones that could be listed—illustrate is how important "myth," unquestioned belief, is in monetary matters. Our own money, the money we have grown up with, the system under which it is controlled, these appear "real" and "rational" to us. The money of other countries often seems to us like paper or worthless metal, even when the purchasing power of individual units is high.

REMEMBER

Money does not actually exist. It's merely an idea. Yes, we have coins and bills that *represent* money, but they are not the actual money itself, and they have little or no intrinsic value. Without the belief in the underlying promise behind money, the physical representation has no value, as the people of Zimbabwe discovered in 2008.

Money is belief

Money, then, is all about belief. The physical representations of money that we grow up with make perfect sense to us. Other representations feel like "play money."

Marco Polo was stunned to discover, on his journey to China, that the Great Khan used *alchemy* — magic, in effect — to (as one chapter title in Polo's book puts it) "*Causeth the Bark of Trees, Made Into Something Like Paper, to Pass for Money All Over his Country*." That's right, surely only magic could turn paper into money!

In fact, even most of your own fiat currency is made of nothing more than an idea. Historian Yuval Noah Harari, in his book *Sapiens*, explains that money is merely an idea, a human concept, not an actual thing you can see or touch.

In fact, he says, "the total value of money worldwide is $60 trillion dollars, of which a mere $6 trillion is in cash or coins 90 percent of all money is nothing more than entries in a computer server. Money is a faith-based object, whose value is derived by the shared narrative about its worth."

You can see this for yourself. If you do an Internet search for "money supply" and dig around a little, you'll find different measures of money supply: M0, M1, M2, and so on. M0 is cash — coins and bills. M1 also includes deposits in checking accounts. M2 includes all that, but also includes savings accounts, mutual funds, and so on. Dig around a little more, and you'll find that what you think of as money — the coins and bills — actually represents only around 10 percent of all the money in circulation!

So, here's a quick question for you. What's the difference between Bitcoin and U.S. dollars, or pounds sterling, or euros? With those fiat currencies, 90 percent of the money is "nothing more than entries in a computer server." With Bitcoin, it's 100 percent!

REMEMBER

There are other differences, of course (some of which we cover in Chapter 2). But our goal here is to show you that Bitcoin and fiat currencies share an important characteristic: They all rely on belief to function. As long as people believe in *any* currency, the currency holds value.

That's not to say any particular currency — including Bitcoin — will hold peoples' beliefs forever. What we are trying to do here is explain how something as ephemeral as Bitcoin can be valuable.

Understanding Bitcoin Benefits

Now that you understand how Bitcoin *can* have value — and clearly it does right now, as millions of people are willing to pay for it — let's take a look at some of the benefits of Bitcoin, characteristics that set it apart as a form of money.

First, consider the roles that money plays:

- Money can act as a **medium of exchange**. That is, you can use it to buy things. Bitcoin currently doesn't do well on this account, because it's not widely accepted, transactions are generally slow and expensive, and most people are still

buying and accumulating Bitcoin for speculative purposes, to see if the value will go up.

- Money can also be a **measure of value** or a **unit of account.** We use it to assign a value to things, from sugar to motor cars. Bitcoin also doesn't do well in this area at the moment because its price is so volatile.
- Money can also act as a **store of value**, a way to take value you have saved and store it away safely. You should be able to buy Bitcoin and let it store your wealth for you, then retrieve it when you need it. Bitcoin has actually done very well in this way over the long term. Certainly, there are short-term fluctuations, but over the long term, due to significant appreciation in value, it's acted very well as a store of value.

Here then, are various characteristics and benefits that set Bitcoin apart.

Portability

Money needs to be portable. If you can't move it around, how can you use it? It may seem that rai stones, from our example earlier in this chapter, were not physically very portable, but in fact their value was definitely portable. The residents of Yap communicated and transferred ownership via word of mouth. Bitcoin is likewise very portable, as you'll discover in this book. You can transmit it across the Internet to anywhere or anyone in the world at nearly the speed of light.

Verifiability

As you see in Chapter 2, your ownership of Bitcoin is most definitely verifiable. Because an entire copy of the Bitcoin blockchain transaction history lives on each computer running the Bitcoin software, the thousands of nodes on the network must verify each and every transaction and block based on the rules of Bitcoin. These are rules that everybody has to follow or they can't function within the network. The structure of the Bitcoin blockchain ensures that you can, and in fact must, prove you own your Bitcoin, and have total control over it before you can

transfer it (assuming you don't lose your private keys; see Chapter 2).

Fungibility

An important characteristic of money is that it has to be *fungible*. That is, one dollar is the same as another, my dollar is just as valuable as your dollar. Like every good form of money, Bitcoin is fungible; every Bitcoin has, in general, the same value as another Bitcoin. (Okay, this isn't 100 percent true. Some people like to own Bitcoin that cannot be traced back through the blockchain to a particular owner. They are willing to pay a bit of a premium for Bitcoin created and transferred without being subject to the kind of Know Your Client banking rules discussed in Chapter 3.)

Durability

Bitcoin won't rot if left out in the weather or burn if your house burns down. Bitcoin is just information, pure money without the vulnerable tangible material. As long as the Bitcoin blockchain and Bitcoin network endure, your Bitcoin will remain where it's always been: in the blockchain. You just have to understand how to protect your access to the blockchain address associated with your Bitcoin, which we discuss in Chapter 5.

Divisibility

Bitcoin can be divided into tiny, tiny parts — one hundred millionths, known as Satoshis. This means you can spend a Bitcoin or any fraction of a Bitcoin. At the current price, the smallest fraction of a Bitcoin is worth about a twentieth of a U.S. cent.

Open access

The Bitcoin network, like the rai stones of the past, is an openly accessible network that cannot be censored. While Bitcoin may not be for everyone, it is for anyone who chooses to use it; no one can limit another's access to the network.

Final settlement

Monetary networks of the past have achieved settlement well; even in the case of the sunken rai stone, the ledger was updated and settlement occurred — albeit via word of mouth. With Bitcoin, transactions can be mathematically irreversible within six confirmations (explained in Chapter 3), which takes about an hour. Compared to other methods, the Bitcoin network provides fairly fast finalized settlements that cannot be charged back.

Borderless, stateless

Bitcoin is international. Any citizen of any country that has open access to the Internet can own and trade Bitcoin. Even if a country tries to ban Bitcoin, the cryptocurrency will continue elsewhere, and knowledgeable citizens would likely be able to bypass restrictions and hide their tracks. A Bitcoin transaction can even be transferred via ham radio, local mesh networks, and satellites.

Pseudonymous

Bitcoin is not, contrary to popular belief, anonymous. But it is *pseudonymous*. The blockchain itself has no account names, for instance. Your Bitcoin is not labeled with your name or any identifying information. (You learn how the blockchain works in Chapter 2.) But the blockchain is open to viewing by the public. Anyone can get in and dig around, and trace transactions from one address to another, to another. This means that if information exists identifying your "entry" into the blockchain — for instance, when you buy Bitcoin from an exchange following KYC (Know Your Customer) banking regulations — your transactions can be traced.

Monopoly-resistant

Bitcoin resides in the peer-to-peer Bitcoin blockchain, which is run by tens of thousands of people. No one person or group of people can seize control.

Debasement-proof

To *debase* means to "reduce (something) in quality or value; degrade." In the context of currency, it originally meant to lower the value of the metal used in coinage. Today, currency debasement typically refers to a government printing more of it, thus making each bill or coin worth less.

An undercurrent of libertarianism runs through the Bitcoin community. One of the big benefits of Bitcoin touted by Bitcoin true believers is that Bitcoin is *not* under the control of any particular government. It's money for the people, by the people.

This means no government — or other form of governing body — can "print" more Bitcoin. In fact, the mathematics that define how Bitcoin works have "baked in" a regular flow of Bitcoin coming into circulation (6.25 Bitcoins every ten minutes currently); every four years, that rate will drop by half, until eventually, the flow of new Bitcoin will dribble away to nothing. Bitcoin cannot be "debased" by flooding the market with more Bitcoin.