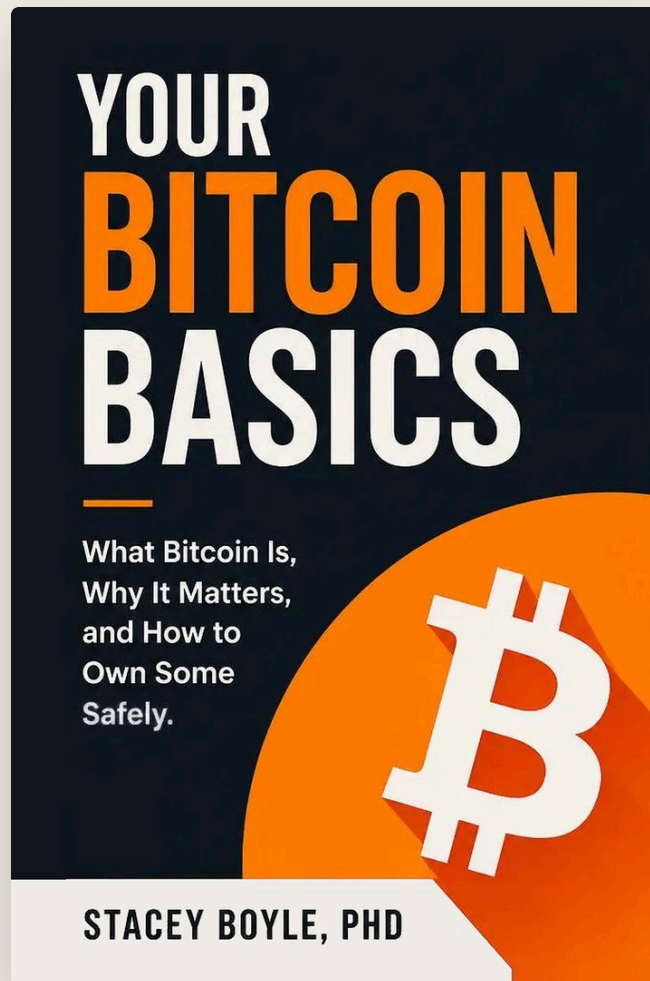




FREE CHAPTER

Chapter 1. Bitcoin made simple

From *Your Bitcoin Basics* by Stacey Boyle, PhD

yourbitcoinbasics.com

From the October 2026 draft. Education, not financial, legal, or tax advice. Copyright 2026 Stacey Boyle. You may print this file and share it whole, free, with credit.

Bitcoin made simple

“The root problem with conventional currency is all the trust it requires to work.”

Satoshi Nakamoto, P2P Foundation forum, February 2009.

By the end of this chapter you will be able to:

1. Give the sixty-second answer to “what is Bitcoin?” in your own words.
2. Explain what a satoshi is and why nobody has to buy a whole one.
3. Sort any digital assets into one of four types.

BEFORE YOU START

There are no wrong answers.

If a friend asked you right now, “What is Bitcoin?”, what would you say? Say it out loud. Notice where you slow down.

Where is the money in your checking account, physically? Who keeps the record of how much is there?

Have you ever owned something you could not touch: airline miles, a song you bought online, a share of a company? What made you confident it was yours?

The sixty-second answer

People ask me what bitcoin is all the time, and I have learned to answer in under a minute, because after a minute they stop listening. Here is what I say.

“Bitcoin is money that no one controls.

The network is a shared ledger of who owns how much, kept in identical copies on thousands of computers worldwide. Because each copy continuously checks the others, the network is decentralized: it has no company, no headquarters, and no boss. No single entity can shut it down or alter it on its own.

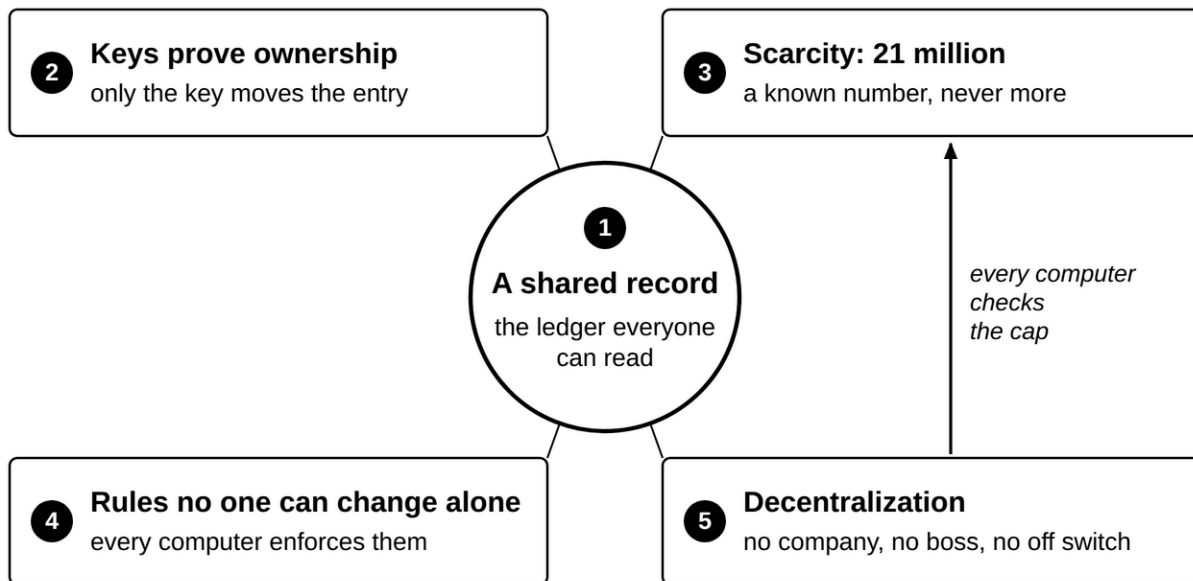
There will only ever be 21 million bitcoin, a fixed limit enforced by mathematics and cryptography. This absolute scarcity is the exact opposite of traditional currencies, which lose purchasing power because governments can always print more.

By combining scarcity with decentralization, Bitcoin is secured by the world's most powerful computer network. It is a global financial system that belongs to everyone who uses it, and to no one in particular.”

That is the whole thing. Everything else in this book is detail, and the details are worth learning, but if you can say that paragraph in your own words, you already know more than most people who argue about it. Whether bitcoin is money yet, in the full sense of the word, is a fair question, and Chapter 7 dives into it.

The six-minute answer: five ideas

When I have more than a minute to explain what bitcoin is, I give the same answer in five parts.



The five ideas of this chapter: a shared record, keys that prove ownership, scarcity (21 million and never more), rules no one can change alone, and decentralization (a network no one owns), which is what keeps the 21 million fixed.

A shared record. Bitcoin is a ledger, meaning a list of entries showing who owns how much, like the ledger a bookkeeper keeps for a business. This one is public and kept in thousands of identical copies. The software lets every copy check every other copy. New entries, or transactions, are added in batches called blocks roughly every 10 minutes, and each block links to the one before it. That chain of blocks is the [blockchain](#).

Keys that prove ownership. Every entry on the ledger is locked. The lock opens with a [private key](#), a very long secret number your wallet keeps for you, like a house key cut to open one door. Whoever holds the key can move the entry. Nobody else can. The ledger does not know your name. It only knows the lock, and only your key opens it. Math (cryptography) protects each entry, and the computing power behind the network protects the ledger's history.

Scarcity: 21 million and never more. New bitcoin is created on a schedule written into the rules in 2009. Each new block pays a reward in new bitcoin to whoever added it to the ledger, a computer owner called a miner (Chapter 4 explains mining). For the first 210,000 blocks, about four years, the reward was

50 bitcoin per block, which created 10.5 million. Then the reward was cut in half, to 25, and the next four years added 5.25 million. It halves again about every four years: 2.625 million, then about 1.3 million, and so on. Each batch is half the one before, so the total creeps toward 21 million and never passes it. The last new bitcoin is expected around the year 2140. About 20.1 million existed as of September 2026.¹ The dollar has no such number. Chapter 3 will show you what that has meant for savers. Scarcity means there is less of something than people would like, and no way to make more on demand. Gold is scarce because digging is hard. Bitcoin is scarce because the rules set the number, and thousands of computers enforce them.

Rules no one can change alone. The ledger's rules live in software anyone can read, and every computer running that software enforces the same rules on every entry. If someone wants to change a rule, every one of those computers would have to agree to run the change. In practice, that has happened only for changes almost everyone wanted, and never for the supply. Chapter 4 shows you how the disagreement gets settled without a boss, referee, or judge.

Decentralization: a network no one owns. There is no Bitcoin company, no headquarters, no chief executive, no customer service line, no marketing department, no bank holiday, no off switch. *The people who write the software don't control the network, and the people who run the computers don't control the software.* The founder left in 2011 and has not been heard from since.² I know how strange that sounds. Chapter 4 is where it starts to make sense. Decentralization means there is no central point of failure: no company to subpoena, no server to unplug, no board to pressure. The record lives everywhere at once, which is why it lives at all. The network is what protects the 21 million. The 21 million cap is one of the rules every computer running the software checks, and every copy of the ledger rejects a block that pays its miner one satoshi too many. Scarcity holds because no one can change it.

The nine-page whitepaper that started it all

On October 31, 2008, someone using the pseudonym Satoshi Nakamoto posted a 9-page paper to a mailing list for cryptographers.¹² The title was “Bitcoin: A Peer-to-Peer Electronic Cash System.” It was about six weeks after Lehman Brothers collapsed and the banking system nearly went with it. The paper is written in plain English; it is free at bitcoin.org, and you can read it in 20 minutes. A whitepaper, in this sense, is a short-published proposal that describes a problem and a design for solving it.

The problem it names is *trust*. Every online payment, Satoshi wrote, has to pass through a bank or a card company, which can reverse it, refuse it, or fail. The sentence that matters is in the first section: “What is needed is an electronic payment system based on cryptographic proof instead of trust.”³ Everything in the paper serves that one sentence.

The design of the Bitcoin network is explained in 12 short sections. You will learn five ideas. A coin is a chain of signatures (Section 2). A timestamped chain of blocks keeps entries in order (Section 3). Computing work makes the chain expensive to fake (Section 4). Computers follow the chain with the

most work behind it (Section 5). A reward of new coins pays the people doing the work (Section 6). Chapter 4 walks through those five sections. The paper ends with the math showing that an attacker trying to rewrite the record falls further behind the longer everyone else keeps working.

Two things the paper does not contain. It never gives a supply cap; the 21 million lives in the software, released in January 2009. And it never uses the word “blockchain,” or “satoshi” as a unit, or “UTXO.” Those words came later, from the bitcoin community. The Worth Repeating note at the end of this chapter explains why that matters.

Who is Satoshi Nakamoto

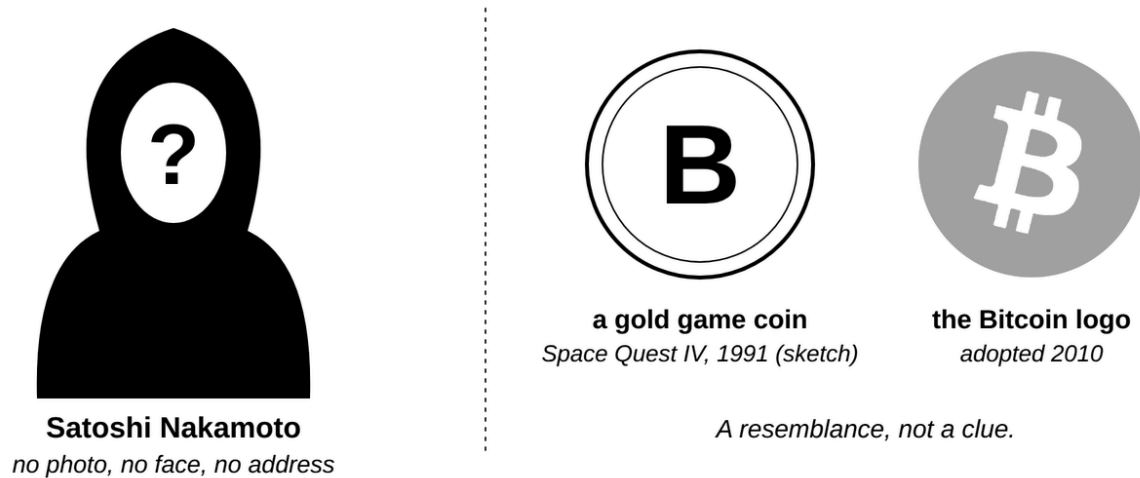
Satoshi Nakamoto is a name, and that is nearly all anyone knows. The name posted the paper in 2008, mined the first block on January 3, 2009, and released the software to the public on January 9, with a newspaper headline about a bank bailout embedded as a timestamp.¹³ The first transaction, on January 12, went to Hal Finney, a programmer in California who had spent a decade on the problem Bitcoin solved.¹⁴ Satoshi wrote on forums and by email for about two years, answered questions patiently, argued with critics, fixed bugs, and then, in April 2011, wrote to a developer that he had “moved on to other things” and disappeared.² Coins that researchers believe Satoshi mined in 2009 and 2010, roughly a million bitcoin, have never moved.¹⁵ As a matter of fact, if you want to prove that you are Satoshi, all you have to do is move a coin on the blockchain. You can only do that if you have the private keys.

Satoshi did not start from scratch. Since 1992, a loose group of cryptographers and programmers calling themselves cypherpunks had been trying to build digital cash that needed no bank.¹⁶ The whitepaper cites two of their proposals directly.³ Satoshi’s contribution was to put the pieces together, add a few new ones so that the network held together, and then hand the project to anyone who wanted to carry it.

Several people have claimed to be Satoshi. The most persistent was an Australian computer scientist named Craig Wright, who spent years suing people who said he was lying. In March 2024, a group of technology companies took him to trial in the High Court of England and Wales. At the end, the judge ruled that Wright is not Satoshi, did not write the whitepaper, and did not create the Bitcoin system. The written judgment in May 2024 described his evidence as forged.¹⁷ *Nobody knows who Satoshi is. For Bitcoin, that is a feature.* No one can arrest, pressure, buy, blackmail, or corrupt a founder.

The hunt has become entertainment in itself. Reporters and filmmakers name a new candidate every few years. In 2014, Newsweek put a retired California engineer named Dorian Nakamoto on its cover; he said he had nothing to do with it. HBO’s *Money Electric: The Bitcoin Mystery* (2024) pointed at the developer Peter Todd, who denied it within hours. *Finding Satoshi* (2026) argued that two early cypherpunks, Hal Finney and Len Sassaman, built Bitcoin together; both died years ago and cannot answer.²⁰ In April 2026, an old theory went viral again: that Bitcoin had been foreshadowed by a 1991 computer game, *Space Quest IV: Roger Wilco and the Time Rippers*. The game’s currency, the buckazoid, is drawn as a gold coin stamped with a B, and internet sleuths stitched the names Satoshi and Nakamoto together from people in the orbit of the game’s publisher. It is a fun afternoon online, and historians of both games and

Bitcoin treat the resemblance as coincidence.²⁰ I tell the story because it shows how badly people want a face to go with the name, and how little the name matters to the network. The ledger works exactly the same whether Satoshi was one person, a group, a government agency, or a 1991 space janitor.



No photo of Satoshi exists. The best-known statue, unveiled in Budapest in 2021, gives the face a mirror finish so visitors see themselves. At right, the kind of game coin that set off a 2026 internet theory, beside the Bitcoin logo.

One more thing Satoshi wrote, in January 2009, when the network was a week old, and a bitcoin was worth nothing: “It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self-fulfilling prophecy.”¹⁸ I quote it for the inspiration. Satoshi was not sure it would work either.

Twenty-one million, and never more

The third idea deserves its own section because it separates bitcoin from every form of money before it. Remember, lowercase “b” means the Bitcoin money, and uppercase “B” means the Bitcoin network.

Gold is scarce because it is hard to dig up. Even so, the world’s gold supply grows by roughly 1.5 to 2% a year as miners find more.⁶ Dollars are scarce only as long as the people who issue them decide they should be, and Chapter 3 shows how that has gone since 1971. Bitcoin’s supply is limited by a rule that every computer on the global network enforces. If a Bitcoin miner tried to award itself more than the schedule allows, every other computer would automatically reject the block as invalid in less than a second. No committee meets. No one votes. The rule simply runs.

People in the Bitcoin world call this a hard asset, meaning something that cannot easily be made more of, like gold and land. The word “hard” is not about the technology. It describes how hard it is to make more. By that measure, bitcoin is harder than anything that came before it, because the answer to “how much more can be made?” is a known number that shrinks toward zero by the year 2140.

I want to be careful here. A fixed supply does not raise the price. The price is set by what people are willing to pay (law of supply and demand), and it has fallen by more than half several times, as Chapter 6 will show with dates. A fixed supply removes one variable from the equation. Whatever bitcoin is worth on any given day, you know that number was not changed by someone printing more.

What a satoshi is

One bitcoin is 100 million satoshis (sats): the Bitcoin logo and, beside it, the 100 million sats it divides into, drawn as a grid of dots.

A dollar divides into 100 cents. *A bitcoin divides into 100 million satoshis, usually shortened to sats.* One satoshi is 0.00000001 bitcoin. The first version of the software in 2009 introduced eight decimals, and the ledger has always counted in the smaller unit.⁴ “Bitcoin” is the display name for 100 million satoshis, the way “a gallon” is a name for a quantity of water and not a thing in itself.

This matters for a practical reason. Nobody has to buy a whole bitcoin, especially at today’s price. You typically buy sats (aka satoshis). If a bitcoin costs \$100,000, a dollar buys 1,000 sats. If it costs \$50,000, a dollar buys 2,000 sats. Any amount in dollars you can afford converts to some number of sats, and the ledger treats a \$10 entry exactly the way it treats a \$10 million one. Beginners often feel that owning less than one whole bitcoin is owning nothing. That feeling has a name: unit bias- judging an amount by the size of the unit instead of by what it is worth. Nobody feels poor holding 50 cents because they lack a whole dollar. The same arithmetic applies here, and Chapter 9 comes back to it when it is time to buy.

It also answers the objection I hear most often in class: “21 million is not enough for 8 billion people.” The objection confuses the number of units with the amount of value. Money doesn’t need many units. It needs units small enough to price a cup of coffee and large enough to price a house. Bitcoin has both. Multiply 21 million bitcoin by 100 million sats, and you get 2.1 quadrillion sats, more than 250,000 for every person on Earth.⁵ Think of a pizza. If more people come to dinner, you do not need more pizza. You cut smaller slices, and each slice is worth more to the person holding it. Bitcoin works the same way. If more people want it, each sat buys more. And if one sat ever became too valuable for small prices, the network could agree to count in smaller pieces. Cutting smaller slices doesn’t add pizza, and adding decimals doesn’t add bitcoin.

Twenty-one million is a small number on purpose. Dividing it is what makes it usable. Satoshi admitted the number was a judgment call. In an April 2009 email to the developer Mike Hearn, he called his choice of the number of coins and the schedule “an educated guess,” picked so prices would land somewhere near existing currencies.²¹ The whole email is on the chapter page on the website.

What a bitcoin actually is

I want to slow down on the first idea, because people get it wrong, and the wrong version causes real confusion later.

A bitcoin is an entry in a ledger. It's not a physical coin. If you looked for the coin itself, you would never find one, because nothing shaped as a coin exists anywhere in the system. Actually, the word bitcoin appears in the whitepaper only in the title. The body never uses it. There is no file on your phone. No picture of a gold B exists anywhere except on the internet.

One ledger entry as a padlock, one private key that fits it, and a list of 12 or 24 plain words, the seed phrase, that can rebuild that key if your signing device (a phone, a computer, or a hardware device) is lost, which is why Chapter 10 will spend so long on those words.

The ledger keeps count more like cash than like a bank balance. Your bank keeps one number for you and adds and subtracts from it. The Bitcoin ledger keeps individual entries, each a specific amount locked to a key, more like the bills in your wallet than the balance on a statement. Chapter 4 shows how an entry gets spent and what the change looks like.

Satoshi Nakamoto described it in one sentence in the whitepaper: “We define an electronic coin as a chain of digital signatures.”³ Each owner signs the entry over to the next. The ledger is the history of those signatures. That is all a bitcoin is.

Bitcoin and “crypto”

When the news says “crypto,” it means a category with millions of things in it. One tracking site counted more than 60 million tokens as of September 2026.⁷ Bitcoin is one of them by that count, and it is the only one this book is about, so I owe you a reason. The reason is easiest to see if you sort the whole category into four types. The sorting question is always the same: *who issued it, and who can change the rules?*

Bitcoin. No issuer. No founder in charge. A fixed supply of 21 million that no one can alter. It launched without a company, without selling tokens to investors first, and without setting aside coins for its creator. It is the only digital asset of any size that fits this description, which is why it gets its own type. Bitcoin came first. Bitcoin is the parent, and cryptos followed.

Altcoins and utility tokens. “Altcoin” means alternative coin: anything built after Bitcoin that copies its general shape. Most have a named founder, a foundation or a company, and a supply the founders can change. Many are utility tokens, meaning tokens you need in order to use a particular platform, like an arcade token that only works in one arcade. Ether, the token of the Ethereum network, is the largest of these. Meme coins, tokens created as jokes or for speculation, sit here too. Some altcoin projects are serious engineering endeavors. All of them have someone who can change the rules, and that is the line that matters. Online you will hear ruder names for them. Whatever the name, it is not bitcoin.

Stablecoins. A stablecoin is a token designed to be worth exactly one dollar, backed by dollars or Treasury bills that a company holds in reserve, like a casino chip that the cashier will always redeem for a dollar. Tether’s USDT and Circle’s USDC are the two largest stablecoins, and the category held roughly \$300 billion in September 2026.⁸ People use them to move dollars across borders in minutes. Their value comes entirely from the issuer (a company) keeping its promise, and the issuer can freeze any token it

wants to. A government can demand the company freezes them too. A stablecoin is essentially a digital dollar offered by a centralized corporation. (A government version, a central bank digital currency, is covered in Chapter 5.) That is the opposite of Bitcoin's design, which is why people who haven't asked the sorting question get them confused.

Tokenized assets. Tokenization means creating a digital certificate of ownership for something that exists elsewhere: gold in a vault, a Treasury bond, a share of a building, a piece of art. The token trades on a blockchain. The thing itself stays where it was, held by a custodian, and the token shows ownership regardless of where the item is stored. Tokenization can make markets cheaper and faster, and large asset managers now sell tokenized Treasury funds.⁹ But a claim is only as good as the party holding the asset, and that party can be sued, hacked, regulated, or shut down. Bitcoin has no custodian to fail, because the ledger entry is the asset.

Here is the sentence I use in class: *the other three types all have someone standing behind them who can change the rules, and Bitcoin has no one like that. Instead, it has the largest and most secure computing network in the world, and anyone can run a copy of the ledger.* That sounds like a weakness until you notice that everyone standing behind an asset can also step away from it. A network cannot step away. It can be abandoned tho.

Your decision. Whether any digital asset other than bitcoin belongs in your life is yours to decide, and a financial advisor can help you weigh it. The tax treatment of stablecoins and tokens varies by case, so ask a CPA or financial expert before you use one. It's best you do your own research too because sometimes traditional finance professionals aren't studied enough on bitcoin and crypto.

Is it a security?

One legal question comes up in every class: is bitcoin a security, like a stock? A security is an investment the law regulates closely, with rules about who may sell it and what they must disclose. In the United States, the answer comes from a 1946 Supreme Court case about a Florida orange grove, SEC v. W.J. Howey Co.¹⁰ The Howey Test asks four questions. Did people invest money? Did they invest it in a common enterprise? Do they expect a profit? Does that profit come from the work of someone else, such as a company or a promoter? If all four answers are yes, the investment is a security. Bitcoin does not meet the fourth: no company sold it to raise money, and no team's work produces its return. Many other tokens meet all four, because a founder sold them to raise money and promised to build something. The Commodity Futures Trading Commission has treated *bitcoin as a commodity*, like gold or wheat, since 2015, and successive chairs of the Securities and Exchange Commission have said it is not a security.¹¹ That legal difference is a large part of why bitcoin was the first digital asset that could be bought inside an ordinary brokerage account through an exchange-traded fund (ETF), which Chapter 13 covers.

THE KITCHEN TABLE

Every chapter contains a kitchen table discussion. This fictional family learns about bitcoin together. Mary is a 76-year-old retired bookkeeper and Alex's mother. Alex is a 51-year-old self-employed concrete contractor and Leisa's father. Leisa is a 27-year-old bankruptcy paralegal who bought her first sats two years ago and is the only one at the table who holds bitcoin on purpose. Mary has \$40 of it on her phone, put there by her granddaughter Emma, Leisa's cousin. The three generations argue about each chapter's topic the way real families do. You will hear your own objection in one of their voices.

Alex: So, Leisa, where is Grandma's \$40? In the phone?

Leisa: The phone has the key. The bitcoin is on the global ledger.

Alex: And where is the ledger?

Leisa: Everywhere. Thousands of computers have a copy.

Alex: So if I hack one of them, I can give myself a million.

Leisa: The other thousands would reject it. That is the whole point of the copies.

Mary: Can I see my entry?

Leisa: Yes. Anyone can. It does not have your name on it, just a code.

Alex: Here is what I don't get. Bitcoin went up last week, and then it crashed. Who decides that? Is it a stock?

Leisa: It is not a stock, Dad. There is no company. A stock is a piece of a company.

Alex: Then what am I buying?

Leisa: An entry on a ledger that no one can print more of.

Alex: And that's worth money because...

Mary: Because your father's dollars are worth less every year, Alex. I was alive for that.

Alex: Fine. But if it's not a stock and it's not a coin, why do they draw a coin on it?

Leisa: Because "an entry in a distributed ledger" is a bad logo.

They got most of it. Leisa's answer to "where is it" is exactly right, and Mary asking to see her own entry is the best question at the table, because she can, and Chapter 4 shows her how. Alex called it a stock, which is the most common mistake I hear from people his age, and Leisa's correction was fair: no company, no share, no dividend. Alex's last question is fair too. The coin on the logo has confused more

people than any scam. When Emma put \$40 of bitcoin on Mary's phone, she created an entry on the public ledger, locked it with a key, and stored the key on the phone. *The bitcoin is on the ledger. The phone holds the key.*

FOR DIFFERENT READERS

By generation. If you kept a passbook at a bank or a checkbook register, you already know what a ledger is; the only new idea is that this one is public, and no one can post to it without a key. If you grew up with shared documents online, think of a spreadsheet that thousands of people can view, and no one can edit except through their own row, with their own password. Both pictures are right. Older readers in my classes tend to trust the ledger faster and the phone slower. Younger readers do the reverse.

Rebuilding your financial life. The ledger has no application form. It does not ask about your credit, your history, or your last address. For someone who has been refused an account, that is the first thing about bitcoin that matters. The ledger also has no customer service, which is why the chapters on keeping it safe come before the chapter on spending it.

WORTH REPEATING

The smallest unit of bitcoin is named after the person who built it, but that person didn't choose the name. In November 2010, a user on the Bitcoin forum named ribuck proposed calling a hundredth of a bitcoin a "satoshi." In February 2011 he suggested the name for the smallest unit instead, and the community settled on it in early 2011, after Satoshi had already stopped posting.¹⁹ The word "blockchain" never appears in the whitepaper either; Satoshi wrote "block chain," two words, and only in later posts.¹² Bitcoin's founder did not even control the vocabulary. The conception and mechanisms of bitcoin came from one person, and the words came from the community, which is what a network with no owner looks like.

DON'T CONFUSE

bitcoin vs Bitcoin

lowercase bitcoin is the money; capital-B Bitcoin is the network and its rules.

the blockchain vs Bitcoin

The blockchain is the technology that keeps the ledger's pages in order; Bitcoin is the whole system: ledger, rules, and network together.

a wallet vs a signing device

A wallet is the app you see, with your balance and a send button; a signing device is whatever holds the private key and approves each payment: a phone, a computer, or a small hardware device. In a phone wallet, the phone is both.

the whitepaper vs the code

The whitepaper is the 9-page proposal from 2008 that explains the design and never mentions 21 million. The code is the software released in 2009 that enforces the rules, including the supply cap and the eight decimals, and it is what the network actually runs.

Satoshi vs a satoshi

Satoshi, capital S, is the founder's name; a satoshi, lowercase, is one hundred-millionth of a bitcoin, named years later by the community.

a stablecoin vs a bitcoin

A stablecoin is a digital dollar with a company behind it that can freeze or redeem it; a bitcoin is an entry on a ledger with no company behind it, and no one who can freeze it.

A FAIR OBJECTION

"If a bitcoin is just an entry in a ledger, how is that different from the number in my checking account? That is an entry in a ledger too."

It is, and the comparison is the right way to understand the difference. Your bank keeps one copy of its ledger. You cannot see the whole thing. Within the law, the bank can edit it, reverse an entry, freeze your entry, or close it. It can also create new entries by lending, which is how most dollars come into existence, as Chapter 3 will describe. You accept all of that because the bank is regulated, insured up to a limit, and someone is there to call.

Bitcoin's ledger has thousands of identical copies, all public. No entry has been changed after the fact since 2010, when a bug let someone create billions of coins, and the network agreed to roll the ledger back- the one exception in its history. No entry can be created outside the schedule. No one can freeze yours. In exchange, there is no one to call. If you lose your private key, the entry stays on the ledger forever, and you can never move it. The bank's ledger gives you a manager and takes away your control and agency over your own money. Bitcoin gives you control and takes away the manager, allowing you to have agency over your own money. That can feel scary, because most of us have never managed our own money without a manager. The chapters ahead are about doing it well.

Try it

Do it on your phone or laptop. The Chapter 1 page at yourbitcoinbasics.com/ch1 has a sats converter and the readable whitepaper.

1. Read the first page of the whitepaper. Open the whitepaper. It is at bitcoin.org, or use the readable web version at yourbitcoinbasics.com/ch1. Read the abstract, which is one paragraph, and the first section, which is half a page. Underline or note every place the word “trust” appears. Skip over any math or tech that confuses you. The network and currency concepts are what matter.
2. Use your device’s find function to search the whole paper for “blockchain.” You will get no results. Search “Satoshi.” You will find it only in the author’s name. Search “21.” Nothing.
3. On yourbitcoinbasics.com/ch1, use the sats converter. Type in what you spend on coffee in a month, or your phone bill. See it in satoshis at today’s price, and notice that the number works fine without a whole bitcoin anywhere in sight.

Check yourself

Check the ones you can do. If one is not there yet, reread that section. It does not mean you failed.

- ☐ I can give the sixty-second answer to “what is Bitcoin?” without notes.
- ☐ I can name the five ideas and say one sentence about each.
- ☐ I can explain what a satoshi is and why 21 million is enough.
- ☐ I can sort a digital asset into one of four types by asking who issued it, and say why this book covers only one.

Scenario. A coworker says, “I just bought some crypto, a coin that’s pegged to the dollar so it can’t crash. Same thing as Bitcoin, right, just safer?” What do you say?

Say or write your answer first. The model response is on yourbitcoinbasics.com/ch1.

The sixteen questions my students ask first

Short answers. Each one names the chapter that goes deeper.

1. Is Bitcoin money for criminals?

Some criminals use bitcoin. Far more use dollars, and every bitcoin transaction sits on a public ledger forever, which is how investigators catch people who thought they were hidden. Chapter 7 has the numbers.

2. What is the difference between Bitcoin and crypto?

“Crypto” is a term for millions of digital tokens, most of which are issued by a company or founder who can change the rules. Bitcoin has no company, no founder in charge, and a supply no one can change; it is the only digital asset (aka cryptocurrency) this book is about. Discussed in Chapter 1.

3. What is the blockchain?

A shared record of who sent how much to whom, kept in identical copies on thousands of computers that check each other, with new entries added in batches called blocks about every 10 minutes. Chapter 4 shows how strangers agree on approving transactions without a boss.

4. How do I buy it?

Small, slowly, and not yet. A phone app takes less time than opening a bank account, but keeping bitcoin safe matters more than buying it, so read Chapters 6, 10, and 11 before you spend a dollar. You can start with ten dollars’ worth; nobody has to buy a whole one. Chapter 9 walks you through the purchase.

5. Who created Bitcoin?

Someone using the name Satoshi Nakamoto published a 9-page paper on October 31, 2008, started the network on January 3, 2009, stopped posting in 2011, and has never been identified. No one is in charge, including the founder. Chapter 1 outlines Satoshi and how Bitcoin came into existence.

6. How many bitcoin are there, and is that enough?

There will only ever be 21 million, and about 20.1 million exist so far. Each one divides into 100 million satoshis, so running out is not the problem. Chapter 1 explains why.

7. What is mining?

Computers worldwide compete to add the next batch of transactions to the record. The competition costs real electricity, and that cost is what makes the record expensive to fake. The miner who wins a new block is paid in new bitcoin. Chapter 4 outlines who the miners are and the mining process.

8. Is bitcoin safe to own? Can it be hacked?

The network has run since 2009 without being hacked, with one early exception in 2010 that was fixed within hours. Companies and apps around it have been hacked many times, and people have been tricked, so keeping bitcoin safe mostly means keeping it away from other people’s mistakes and your own. Chapters 4, 10, and 11.

9. Is it legal?

In the United States, yes. You can buy, hold, spend, and sell it, and the IRS taxes it as property. Some countries restrict it. Chapters 7 and 13.

10. Is it too late to invest in bitcoin?

People have said “too late” at every price for 17 years, and roughly 4% of the world holds any bitcoin at all. You are late, but it’s not where you think. Chapter 6 explains the difference between late and too late.

11. Why does the price fall so hard? Can it go to zero?

The supply is fixed, so every change in demand hits the price, and no central bank smooths it. Bitcoin has fallen more than 75% four times, and nothing in the code prevents it from going to zero. Chapter 6.

12. Isn’t Bitcoin a Ponzi scheme?

No. A Ponzi scheme has an operator who promises returns and pays early investors with newer investors’ money until it runs out. Bitcoin has no operator, promises no return, and pays no one; buyers buy from sellers at a market price. The price can still fall hard. Chapter 8 answers this in full.

13. Where do I keep it?

In a wallet that serves as your signing device that holds your keys rather than your bitcoin. In the book, your options are listed as a ladder that runs from “a fund or an app holds it for me” to “I hold it myself on a device the size of a thumb drive.” Higher is not safer for everyone. Chapter 10 lays out your options.

14. Can I spend it? Can I turn it back into cash?

Yes, to both, and both count as selling for tax purposes. Chapters 12 and 13 explain.

15. Is it taxed?

Holding it is not taxed. Selling, spending, or trading it is taxed on the difference between what you paid and what it was worth, so keep records from the first purchase. See Chapter 13.

16. Isn’t it bad for the environment?

The Bitcoin network uses real energy, roughly half of 1% of the world’s electricity by the most-cited estimate. Whether that is “bad” depends on what powers it and what you think the network is worth. Chapter 4 gives both sides.

Notes for Chapter 1

1. Circulating supply, calculated from block height 969,192 (Blockstream and BlockCypher block explorers, September 29, 2026): about 20.09 million bitcoin of a maximum of 21 million. Because amounts are rounded to whole satoshis, the true maximum is a hair under 21 million, about 20,999,999.98.
2. Satoshi Nakamoto, email to developer Mike Hearn, April 23, 2011 (“I’ve moved on to other things. It’s in good hands with Gavin and everyone.”), as shared by Hearn and reported in Vice (Motherboard), August 11, 2017; last public forum post, bitcointalk.org, December 2010, as archived by the Satoshi Nakamoto Institute (retrieved September 2026).
3. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” bitcoin.org, 2008. Quotations from Sections 1 and 2; citations to Back and Dai in the paper’s reference list.
4. Source code, main.h, 2009: “static const int64 COIN = 100000000;” (earliest version in the bitcoin/bitcoin repository, github.com, retrieved September 2026); the version 0.1.0 release of January 9, 2009 is archived at satoshi.nakamotoinstitute.org/code.
5. Arithmetic: $21,000,000 \times 100,000,000 = 2.1 \times 10^{15}$ satoshis; world population from United Nations World Population Prospects, 2024.
6. World Gold Council, “Above-ground stocks,” gold.org (retrieved September 2026): about 222,600 tonnes as of mid-2026; World Gold Council, Gold Demand Trends, Full Year 2025 (2026): mine production of 3,672 tonnes in 2025, about 1.7% of the above-ground stock.
7. CoinMarketCap, coinmarketcap.com, site-wide count of cryptocurrencies tracked, 62.26 million (retrieved September 2026); CoinGecko, by comparison, listed about 21,700 coins the same month.
8. DefiLlama, “Stablecoins,” defillama.com, total stablecoin market cap about \$306 billion, of which Tether USDT about \$184 billion and Circle USDC about \$75 billion (retrieved September 29, 2026).
9. rwa.xyz, “Tokenized Treasuries,” app.rwa.xyz, about \$14.7 billion across 25 products, including funds from BlackRock (BUIDL), Franklin Templeton (BENJI), WisdomTree, Invesco and JPMorgan (retrieved September 29, 2026).
10. SEC v. W.J. Howey Co., 328 U.S. 293 (1946).
11. Commodity Futures Trading Commission, In re Coinflip, Inc., d/b/a Derivabit, order and press release, September 17, 2015, cftc.gov (retrieved September 2026), finding for the first time that bitcoin and other virtual currencies are commodities; SEC Chairman Jay Clayton, testimony before the House Appropriations Committee, April 26, 2018 (as reported by Coin Center); SEC Chair Gary Gensler, CNBC interview, June 27, 2022 (as reported by Decrypt). No court and no SEC rule has ever held bitcoin to be a security; the CFTC’s commodity finding came in an enforcement order, not a rule; and the market-structure bill that would write the commodity classification into statute, the CLARITY Act, passed the House on July 17, 2025, then stalled in the Senate in September 2026 (Orrick, “The CLARITY Act Stalls in the Senate,” October 2, 2026, orrick.com, retrieved October 2026).
12. Satoshi Nakamoto, “Bitcoin P2P e-cash paper,” posting to the Cryptography Mailing List (metzdowd.com), October 31, 2008 (retrieved September 2026); “block chain” as two words in Satoshi’s later bitcointalk.org posts, e.g. “Checking the block chain on load,” August 16, 2010, as archived by the Satoshi Nakamoto Institute; neither “blockchain” nor “block chain” appears in the whitepaper.
13. Bitcoin block 0, January 3, 2009, containing the text “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”; software release announced January 9, 2009 on the same mailing list.
14. Bitcoin block 170, January 12, 2009, first transaction to Hal Finney; Finney, “Bitcoin and me,” bitcointalk.org, 2013.
15. Sergio Demian Lerner, “The Well Deserved Fortune of Satoshi Nakamoto,” bitslog.com, April 17, 2013 (about 1 million bitcoin mined by a single early entity and never spent); Lerner’s later “Patoshi” analyses put the figure near 1.1 million, as he confirmed in a Cointelegraph Magazine interview (retrieved September 2026).
16. Eric Hughes, “A Cypherpunk’s Manifesto,” 1993; Adam Back, “Hashcash,” 1997 (paper 2002); Wei Dai, “b-money,” 1998; Nick Szabo, “Bit Gold,” 1998 (published 2005); Hal Finney, “RPOW,” 2004.
17. Crypto Open Patent Alliance v. Wright, High Court of England and Wales, ruling announced from the bench March 14, 2024 (CoinDesk, March 14, 2024); written judgment [2024] EWHC 1198 (Ch), Mellor J, May 20, 2024, judiciary.uk (retrieved September 2026).
18. Satoshi Nakamoto, “Re: Bitcoin v0.1 released,” reply to Dustin D. Trammell on the Cryptography Mailing List (metzdowd.com), January 16, 2009 (retrieved September 2026).
19. bitcointalk.org, ribuck, post in “More divisibility required - move the decimal point,” February 10, 2011, proposing “austrian” or “satoshi” for the smallest unit (retrieved September 2026); the earlier proposal, calling 0.01 bitcoin a “satoshi,” was ribuck’s post of

November 15, 2010 in “Official Bitcoin Unicode Character?,” bitcointalk.org topic 369, as dated by the Bitcoin Wiki entry “Satoshi (unit),” en.bitcoin.it, retrieved October 2026.

20. Cullen Hoback, director, *Money Electric: The Bitcoin Mystery*, HBO, October 8, 2024, and Peter Todd's denial the same week, as reported by CoinDesk; Kurt Robson, “Was Bitcoin Discovered in a 1991 Video Game? Inside the Viral Theory Gripping Crypto,” CCN, April 13, 2026 (the buckazoid coin in *Space Quest IV*, Sierra On-Line, 1991; the game's designers were Mark Crowe and Scott Murphy; no documented link to Bitcoin). Leah McGrath Goodman, “The Face Behind Bitcoin,” *Newsweek*, March 6, 2014, and Dorian Nakamoto's denial the same week (*Associated Press*); *Finding Satoshi*, directed by Tucker Tooley and Matthew Miele, released April 22, 2026 (*The Block*, April 2026).
21. Satoshi Nakamoto, email to Mike Hearn, April 12, 2009, published by Hearn and reported in *Vice (Motherboard)*, August 11, 2017; full text archived at [gutenberg.net](https://gutenberg.org) (retrieved October 2026).

Want the rest?

Fourteen more chapters, from how a transaction works to keeping your bitcoin safe and passing it on. Signed copies and group orders: yourbitcoinbasics.com/buy. Every chapter has a free companion page with activities, current numbers, and links: yourbitcoinbasics.com.