



Bitcoin, Explained

A short guide for people who've heard of it
and want to actually understand it.

From The Weekly BOLT — Bitcoin and macro, every Monday. Free.
staybolted.com · First edition, September 2026

Contents

This guide is for the person who knows Bitcoin exists, has maybe owned a little, and has never had it explained in a way that made the whole picture click. Ten short chapters, in order, each ending with the three things worth remembering. Nothing here is investment advice. It's the understanding you need to form your own view — which is the only kind worth having.

01 What money is for

Why money exists, what it has to do, and how the dollar stopped doing it.

02 The problem Bitcoin solves

Digital cash was impossible for forty years. Here is the problem, and the fix.

03 How it actually works

Keys, blocks, miners, and nodes — the mechanism in plain language.

04 21 million

Where the cap comes from and why nobody can raise it.

05 Who's in charge

Developers, miners, and nodes, and what happened when people tried to change the rules.

06 Volatility, and why it looks the way it does

Four crashes, four recoveries, and what the swings actually mean.

07 Bitcoin and the bond market

The chapter BOLT exists for: debt, yields, trust, and where Bitcoin fits.

08 The energy question

What the electricity buys, where it comes from, and the AI comparison.

09 Holding it

Keys, seed phrases, custody — what it means to actually own some.

10 How to keep learning

The questions worth asking, and where to go from here.

Each chapter ends with a **What to remember** box — the three things worth keeping if you keep nothing else.

What money is for

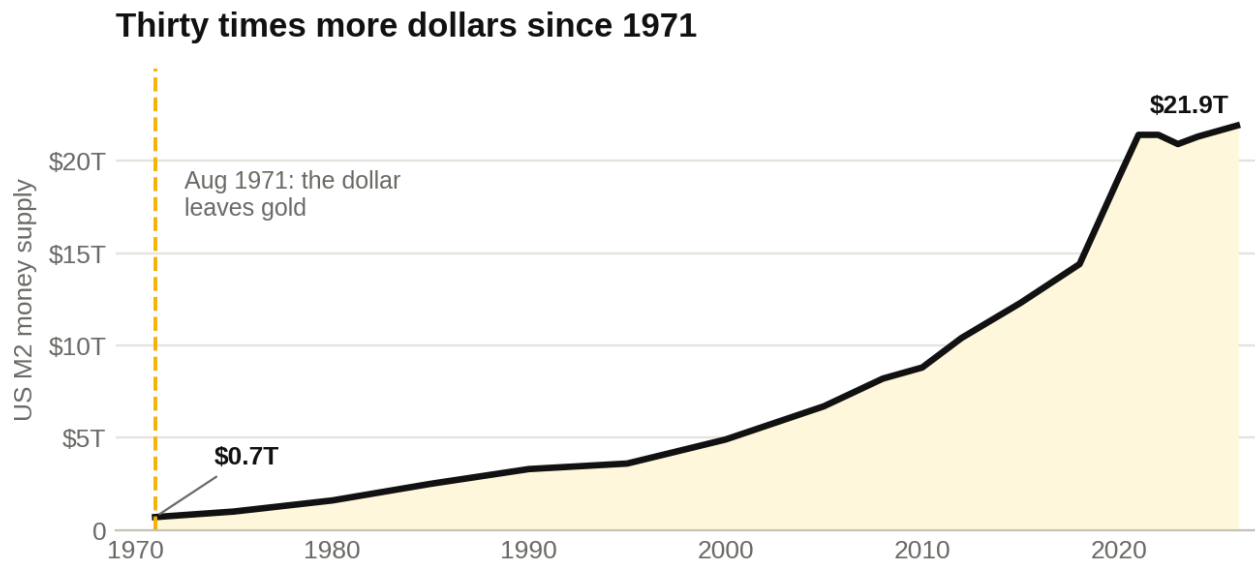
Before Bitcoin makes any sense, it helps to ask a question most people never think about: what is money actually for?

Strip away the paper and the apps and the numbers on a screen, and money does three jobs. It lets you trade without hauling around the thing you make (a **medium of exchange**). It lets you keep the value of today's work for later (a **store of value**). And it gives everyone a common yardstick so a haircut and a bag of groceries can be compared (a **unit of account**). Anything that does those three jobs well is money. Anything that does them badly gets replaced, eventually, by something that does them better.

For most of history, the thing that did them best was gold. Not because anyone voted for it, but because gold has properties that make it hard to beat. It's scarce, and it stays scarce — the world's gold supply grows around 1.5% a year, and no one has found a way to speed that up. It doesn't rot or rust. It can be divided into small pieces and melted back into large ones. And it's hard to fake. Societies that tried other things — seashells, tobacco, iron bars, tulips — kept drifting back to the metal, because whatever they used instead was either too easy to make more of or too hard to move.

That "too easy to make more of" part is the one that matters most. Money only works as a store of value if the person holding it can trust that there won't be a lot more of it tomorrow. Every time a ruler figured out how to shave a little silver off the coins, or a government figured out it could print notes faster than it could back them, the money got worse at its job and people got quietly poorer. The word for this is **debasement**, and it's as old as money itself.

What changed in 1971



Source: Federal Reserve (FRED, M2SL). Values approximate, as of September 2026.

For a long stretch of the 20th century, the dollar was tied to gold. After World War II, the world's major currencies were pegged to the dollar, and the dollar was redeemable for gold at \$35 an ounce. That arrangement — called Bretton Woods — meant that even if you never touched gold, the money in your pocket was anchored to something that couldn't be printed.

On August 15, 1971, President Nixon ended that. The United States stopped converting dollars to gold, temporarily at first, then permanently. From that point on, the dollar — and every currency pegged to it — was backed by nothing but the government's word and the market's confidence. Economists call this **fiat** money, from the Latin for "let it be done." It is money because someone with authority says it is.

This isn't a conspiracy story; it was a policy choice, and a defensible one at the time. But the consequence is easy to see in the numbers. In 1971 the U.S. national debt was about \$400 billion. Today it's past \$37 trillion. The supply of dollars in circulation (M2) has grown from roughly \$700 billion to over \$21 trillion. A house that cost \$25,000 in 1971 costs \$400,000 today. The house didn't get sixteen times better. The yardstick got shorter.

That's the environment Bitcoin was born into: a world where every major currency can be created at will, where the people creating it face real pressure to create more, and where the tool for measuring value is itself losing value. It's not that the dollar is about to collapse. It's that a lot of people have started asking a question that used to have an obvious answer: *what is money supposed to be, and is this it?*

Why it matters that the question came back

Here's the thing to hold onto from this chapter. For fifty years, the answer to "what is money" has been "whatever the central bank says." That worked well enough when governments ran modest deficits and interest rates could go up and down freely. It works less well when debt is 120% of GDP and every rate hike adds hundreds of billions to the interest bill — which is where the United States is now, and why the bond market has started behaving in ways the textbooks don't predict. (We write about this every week.)

Bitcoin's pitch, at its simplest, is this: what if money could have gold's scarcity without gold's weight — something no one could print, that you could send across the world in minutes, and that didn't need anyone's permission? That's a new idea. The next chapter is about why, until 2009, it wasn't possible.

What to remember: Money does three jobs — spending, saving, measuring — and it does them well only when nobody can make more of it easily. Since 1971, no major currency has that property. That's the gap Bitcoin was designed to fill.

The problem Bitcoin solves

Everything digital can be copied. That's the whole point of computers. Send someone a photo and you both have the photo. Email a spreadsheet and there are now two spreadsheets. It's the reason the internet works and the reason digital money was, for decades, considered impossible.

Think about what a dollar in your bank account actually is: a number in a database. If you could copy that number the way you copy a photo, you'd be rich and the dollar would be worthless. So we don't let you. A bank sits in the middle, keeps the one true copy of the ledger, and when you pay someone, the bank subtracts from your row and adds to theirs. Visa, PayPal, Venmo — same idea. Every digital payment you've ever made ran through somebody's database, and that somebody decided whether it went through.

This works. But it means digital money has always required a trusted middleman, and that middleman has power: to freeze your account, to charge a fee, to report you, to go bankrupt with your money inside, to be told by a government which transactions to block. Cash doesn't have that problem. Hand someone a \$20 bill and it's done; no one approved it, no one can reverse it, and you don't have the bill anymore. For a long time, "cash but digital" seemed like a contradiction.

The double-spend problem

Computer scientists had a name for this: the **double-spend problem**. If I have one digital coin and I send it to Alice, what stops me from also sending the same coin to Bob? Without a central ledger to check against, both Alice and Bob would see a valid-looking payment. The coin has been spent twice. Any digital money without a middleman would collapse the moment someone figured this out — and someone always would.

People tried. Through the 1990s and 2000s, a loose community of cryptographers and programmers built one attempt after another: DigiCash, e-gold, b-money, Bit Gold, Hashcash. Each solved a piece of the puzzle. None solved the whole thing. They either kept a company in the middle (and the company got shut down or went under), or they had no way to stop double-spending without one.

The 2008 answer

On October 31, 2008 — six weeks after Lehman Brothers collapsed — someone using the name Satoshi Nakamoto posted a nine-page paper to a cryptography mailing list. The title was plain: *Bitcoin: A Peer-to-Peer Electronic Cash System*. The first sentence stated the goal: a version of electronic cash that would let payments go directly from one party to another "without going through a financial institution."

The insight was to flip the problem around. Instead of one trusted party keeping the one true ledger, what if *everyone* kept a copy of the ledger, and there was a way to agree on which copy was right that didn't require trusting anyone in particular?

That's what Bitcoin is: a single shared record of who owns what, copied onto thousands of computers around the world, updated in batches roughly every ten minutes, with a set of rules that make it enormously expensive to lie and free to verify. If I try to send the same coin to Alice and to Bob, the network sees both, accepts one, and rejects the other — and there's no company to call and no server to hack, because there isn't one. The middleman has been replaced by math and electricity.

The software went live on January 3, 2009. Embedded in the very first block was a newspaper headline from that morning: *"Chancellor on brink of second bailout for banks."* Whoever Satoshi was, they wanted the timing on the record.

Why "nobody in the middle" is the point

It's easy to hear all this and think the achievement was technical. It was, but the reason it matters is not technical. Removing the middleman means removing the middleman's power. Nobody can freeze a Bitcoin account, because there are no accounts — just keys. Nobody can print more, because the rules are enforced by every participant, not decreed by one. Nobody can be told which payments to block, because there's nobody to tell.

For someone in the United States with a working bank, that can sound abstract. For the roughly 1.4 billion adults with no bank account, for anyone who's watched their currency lose half its value in a year, for anyone whose government has decided their savings belong to it — it's not abstract at all. And, as the last chapter argued, the question of whether the people running the money can be trusted to run it well has recently gotten a lot less abstract in the United States too.

What to remember: Digital things can be copied, so digital money always needed a bank in the middle to keep the one true ledger. Bitcoin's breakthrough was a shared ledger that everyone keeps and no one controls, which makes double-spending impossible without a middleman. The technical trick matters because of what it removes: anyone's power to stop, reverse, or dilute your money.

How it actually works

You don't need to understand the machinery to use Bitcoin, any more than you need to understand TCP/IP to send an email. But most of the confident-sounding nonsense about Bitcoin comes from people who skipped this part, so it's worth twenty minutes. We'll use one running picture: a small town with a shared notebook.

The notebook

Imagine a town where nobody uses cash. Instead there's a notebook, and every payment gets written in it: "Maria pays Sam 5." To know how much anyone has, you read the whole notebook and add it up. Nobody has a "balance" stored anywhere; they just have every entry that ever mentioned them.

Now imagine that instead of one notebook in the town hall, every household keeps an identical copy. When Maria pays Sam, she announces it to the whole town, and everyone writes it into their own notebook. If Maria tries to pay Sam and Bob with the same 5, everyone sees both announcements, and the rule is simple: the first one you hear counts, the second is ignored.

That's the Bitcoin ledger. The households are **nodes** — computers running the Bitcoin software, of which there are tens of thousands worldwide. The notebook is the **blockchain**. And an "entry" is a **transaction**. There are no accounts; there are only signed entries saying that coins previously sent to one key are now being sent to another. (If you want the technical version of this — the "UTXO model" — there's a Bitcoin Bite on it.)

Keys, not passwords

How does the town know it was really Maria who announced the payment? Every person holds a **private key**, a very large random number that only they know, and a matching **public key** that everyone can see. When Maria writes "Maria pays Sam 5," she signs it with her private key. Anyone can check the signature against her public key and confirm it's authentic — without ever learning the private key itself. This is the same public-key cryptography that secures your bank's website; Bitcoin just uses it for ownership instead of login.

The important consequence: whoever holds the private key holds the coins. Not the person who "should" own them, not the person whose name is on something — the key. That's why the Bitcoin world repeats "not your keys, not your coins" until it's tiresome, and why Chapter 9 is about keeping them safe.

Who writes the next page

Here's the hard part. If everyone keeps a copy, and announcements arrive in slightly different orders in different parts of town, how does the town agree on the official order? Which copy of the notebook is right?

Bitcoin's answer is that the notebook is written in **pages** — called blocks — and only one household gets to write each page. Every ten minutes or so, one node wins the right to bundle up all the recent announcements into a block, and everyone else copies that block into their notebook. The winner is chosen by a contest that's deliberately expensive to enter.

The contest is called **mining**, and the expense is called **proof-of-work**. Nodes that want to write the next block — miners — race to find a number that, when combined with the block's contents and run through a scrambling function, produces an output below a certain target. There's no shortcut; the only way to find the number is to guess, trillions of times a second, until you get lucky. It's like a lottery where you buy tickets with electricity. The first miner to hit the target broadcasts the block, everyone checks it in a fraction of a second (checking is easy; only finding is hard), and if it's valid, it becomes the next page.

The winner gets paid — currently 3.125 newly created bitcoin per block, plus the fees attached to the transactions inside. That's how new bitcoin enters circulation, and it's the *only* way. There's no other faucet.

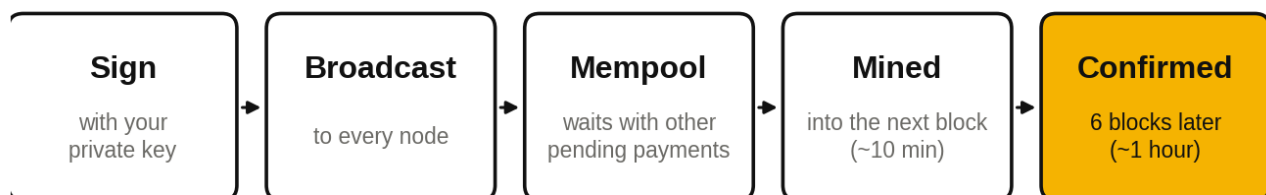
Why the waste isn't waste

People ask why Bitcoin burns all that electricity when a bank does the same job with a database. The answer is that the electricity is the security. Because writing a page costs real-world resources, rewriting history costs even more. If someone wanted to alter a transaction from an hour ago, they'd have to redo the work for that block *and every block since*, faster than the entire rest of the network is adding new ones. With the network today running above a zettahash — a thousand billion billion guesses per second — no government or company on earth has the hardware to do it. That's not a claim about intentions; it's arithmetic.

This is also why Bitcoin is slow on purpose. Ten minutes per block is a design choice that gives every node time to hear about the new page before the next one is written. And it's why the network adjusts. Every 2,016 blocks — about two weeks — the difficulty of the puzzle is recalibrated so blocks keep arriving every ten minutes no matter how many miners join or leave. More miners, harder puzzle. Fewer, easier. The schedule holds.

Putting it together

A payment's journey: nobody approves it, and nobody can undo it



Maria signs a payment with her private key. She announces it. It sits in a waiting area (the **mempool**) alongside everyone else's pending payments. A miner picks it up, wins the block, and writes it into the shared notebook. Every node checks the block and adds it. Six blocks later — about an hour — it's buried under enough work that reversing it is, practically, impossible. Nobody approved it. Nobody can undo it. Sam has the coins.

That's the whole system. Everything else — wallets, exchanges, ETFs — is built on top of this, and none of it changes it.

What to remember: Bitcoin is a shared ledger that thousands of computers keep identical copies of. Ownership is proven by private keys, not by accounts. Every ten minutes, miners compete — by spending electricity on a guessing game — to write the next page, and that expense is what makes the history permanent. New coins come only from that process, on a fixed schedule.

CHAPTER 4

21 million

There will never be more than 21 million bitcoin. Almost everyone who's heard of Bitcoin has heard that number. Fewer people know why it's credible, and that's the part worth understanding — because "a company promised" and "the rules of the system make it so" are very different kinds of promise.

The schedule

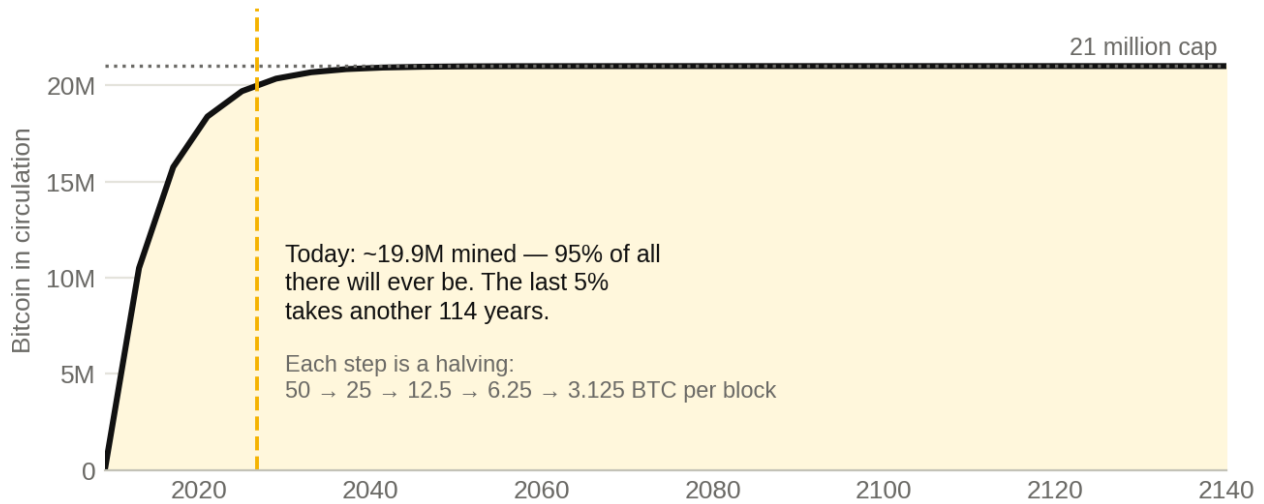
New bitcoin enter circulation one way: as the reward paid to the miner who writes each block. When the network launched in 2009, that reward was 50 bitcoin per block. The rules say that every 210,000 blocks — roughly every four years — the reward is cut in half. It went to 25 in 2012, 12.5 in 2016, 6.25 in 2020, and 3.125 in April 2024. The next cut, to 1.5625, is expected in 2028.

Halve something enough times and it approaches zero. Add up every reward that will ever be paid and you get a hair under 21 million, with the last fraction of a coin mined somewhere around the year 2140. Today, about 19.9 million already exist — roughly 95% of all the bitcoin there will ever be. The remaining 5% arrives over the next 114 years, at a slower and slower drip.

Compare that to gold, whose supply grows about 1.5% a year, or the dollar, whose supply has grown about 7% a year on average since 1971 and far faster in some years. Bitcoin's supply grows under 1% a year right now, and that rate only falls. It is the first money in history whose future supply is known, to the coin, in advance.

Why "just make more" isn't possible

The only money whose future supply is known in advance



Computed from the Bitcoin issuance rules: 50 BTC per block, halving every 210,000 blocks (~4 years).

This is where people get skeptical, reasonably. Rules can be changed. Software can be updated. Who's to say a future version of Bitcoin doesn't lift the cap to 42 million?

The answer is: anyone *could* write that software. Getting anyone to run it is the problem. Remember the town from Chapter 3: every household keeps its own copy of the notebook, and every household checks every new page against the rules it already has. If a miner writes a block that pays itself 100 bitcoin instead of 3.125, every node rejects that block. Not by vote, not by committee — automatically, because it doesn't follow the rules the node was told to enforce. The miner has burned electricity to produce a page nobody will copy.

To raise the cap, you wouldn't need to convince a company or a government. You'd need to convince the tens of thousands of people running nodes to voluntarily install software that makes the bitcoin they already hold worth less. Every one of them has the opposite incentive. This is the difference between Bitcoin and everything before it: the supply limit isn't a policy that someone enforces. It's a property that everyone enforces on everyone else, because doing so is in their own interest.

Could the rules change in other ways? Yes, and they have — but only through changes that the overwhelming majority of the network agrees to run, which in practice means changes that make Bitcoin more useful without touching what makes it valuable. Chapter 5 is about how that actually plays out, including a proposal this summer that failed for exactly this reason.

Scarcity you can verify

One more thing that makes the 21 million different from gold's scarcity. Nobody knows precisely how much gold exists. Estimates for all the gold ever mined range across tens of thousands of tons, and a new discovery or a cheaper extraction method can change the picture. Bitcoin's supply, by contrast, can be checked by anyone, at any moment, to the satoshi (a hundred-millionth of a bitcoin), by running a node and adding up the ledger. There's no audit to trust. You just count.

That auditability matters more than it sounds. Much of the history of money is the history of people discovering, too late, that there was more of it than they'd been told — coins clipped, reserves overstated, promises of gold backing that weren't kept. Bitcoin is the first money where "how much is there" has a single, public, verifiable answer.

What scarcity does and doesn't mean

Scarcity alone doesn't make something valuable; plenty of rare things are worthless. What scarcity does is make Bitcoin *capable* of being a store of value in a way that things with elastic supply can't be. If demand rises for dollars, more dollars appear. If demand rises for bitcoin, the price rises and the supply doesn't move — the same dynamic that made gold the world's savings vehicle for a few thousand years, in a form you can send over the internet.

Whether demand *does* rise is a separate question, and it's the one the rest of this guide — and every issue of BOLT — is really about.

What to remember: New bitcoin are created only as mining rewards, and the reward halves every four years, which caps total supply at 21 million with about 95% already issued. The cap holds not because anyone promises it but because every node enforces it and every holder has reason to keep it that way. It's the first money whose supply is fixed, known in advance, and verifiable by anyone.

Who's in charge

Nobody. That's the short answer, and it's the one that makes people uneasy, because everything else in their financial life has someone in charge. A bank has a CEO. The dollar has the Federal Reserve. Even a company like Apple has a board you could, in principle, write a letter to. Bitcoin has none of that — no founder who's around (Satoshi stopped posting in 2011 and has never been identified), no headquarters, no board, no customer service line.

What it has instead is three groups of people whose interests overlap but don't align perfectly, and a set of rules that only change when all three agree. Understanding how those groups check each other is the difference between "Bitcoin is anarchy" and "Bitcoin is the most stable set of monetary rules in the world."

The three groups

Developers write the software. Most of them contribute to Bitcoin Core, the reference implementation, through a public process anyone can read. They can propose changes, but they can't impose them; a developer who commits a change nobody wants to run has changed nothing. Their power is the power to suggest.

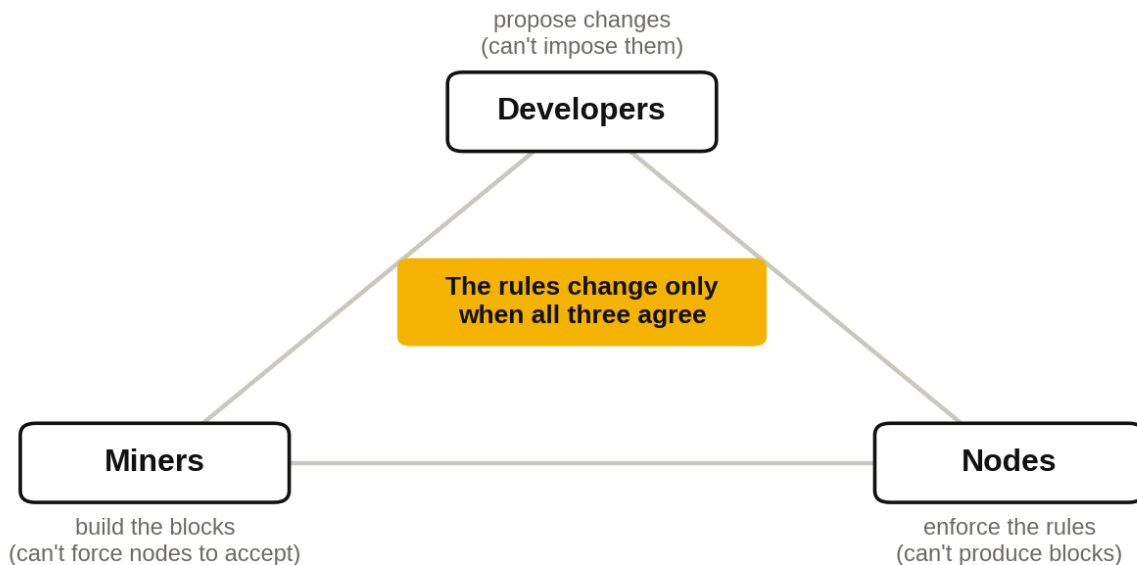
Miners write the blocks. They choose which transactions to include and which version of the rules to build on. If enough miners started building blocks under a new rule, they could force the question — but only if the third group went along. A block that nodes reject is worthless, and miners have millions of dollars in hardware whose entire value depends on producing blocks that nodes accept. Their power is the power to extend the chain.

Nodes — the tens of thousands of people running full copies of the ledger — enforce the rules. Every block gets checked against the rules that node was told to follow, and anything that breaks them is thrown out, no matter who mined it or how much work went in. Node operators include exchanges, businesses, and a great many individuals running a small computer in a closet. Their power is the power to say no.

No group can move without the others. Developers can't force miners to mine their code. Miners can't force nodes to accept their blocks. Nodes can't produce blocks at all. The result is a system where changing the rules requires something close to unanimous consent — and where the safest change is always no change.

The 2017 lesson

Nobody's in charge: three groups that check each other



The clearest demonstration came in 2017. Bitcoin was congested; fees were high. A large group of businesses and miners — representing well over 80% of the network's mining power — backed a plan to double the block size, which would have let more transactions through. They announced it as a done deal.

It wasn't. Node operators and users, who'd had no seat at the table, simply declined to run the new software. When it became clear that the coins produced under the new rules wouldn't be recognized by the exchanges and users who mattered, the plan was abandoned before it activated. The people with the most hashpower and the most money lost to the people with the most nodes. A separate group did fork off to create a larger-block coin, which still exists and is worth a small fraction of Bitcoin. The market decided which rules were Bitcoin.

The 2026 lesson

It happened again this summer, in a smaller way that made the same point. A proposal called BIP-110 aimed to temporarily restrict how much non-financial data could be stuffed into transactions — the images and tokens that had been bloating the chain since 2022. Supporters felt it protected Bitcoin as money; critics saw it as a form of censorship with real risk of splitting the network. The proposal set an unusually low bar for activation, 55% of miners signaling support, and included a fallback that would force the issue if that bar wasn't met.

Miner support came in at 2.5%. When the deadline hit, the handful of nodes running the fallback rejected the next block and split onto their own chain — which produced two blocks, stalled, and fell a hundred blocks behind while the real network carried on without noticing. The proposal was reasonable, the debate was serious, and the answer was still no. That is how Bitcoin says no: not with a vote, but with the quiet refusal of enough people to run the code.

Why this is the feature

It would be easier, in some ways, if Bitcoin had a board that could fix things. Fees could be lowered by decree. Mistakes could be reversed. But a board that can lower fees can also raise the supply cap, freeze an address, or reverse a transaction that a powerful person wants reversed — and once that power exists, it will be used. Every money that had someone in charge eventually had that someone act in their own interest. The whole reason Bitcoin is worth anything is that there's nobody to pressure, nobody to bribe, nobody to subpoena, and nobody who can be persuaded that just this once, the rules should bend.

The cost of that is slowness. Improvements take years. Debates get ugly. Some good ideas never happen. Bitcoin's supporters have decided that's a price worth paying for money whose rules can't be changed by the people it's inconvenient for. You don't have to agree. But it's important to see that it's a choice, not an accident.

What to remember: Nobody runs Bitcoin. Developers propose, miners build, and nodes enforce, and the rules change only when nearly everyone agrees. Twice — in 2017 and again in 2026 — well-organized attempts to change them failed because ordinary node operators declined to go along. That resistance to change isn't a bug in the governance; it's the reason the 21 million cap can be trusted.

Volatility, and why it looks the way it does

If Bitcoin is supposed to be sound money, why does its price swing 10% in a week? It's a fair question, and the honest answer has two parts: it's true, and it's what you'd expect.

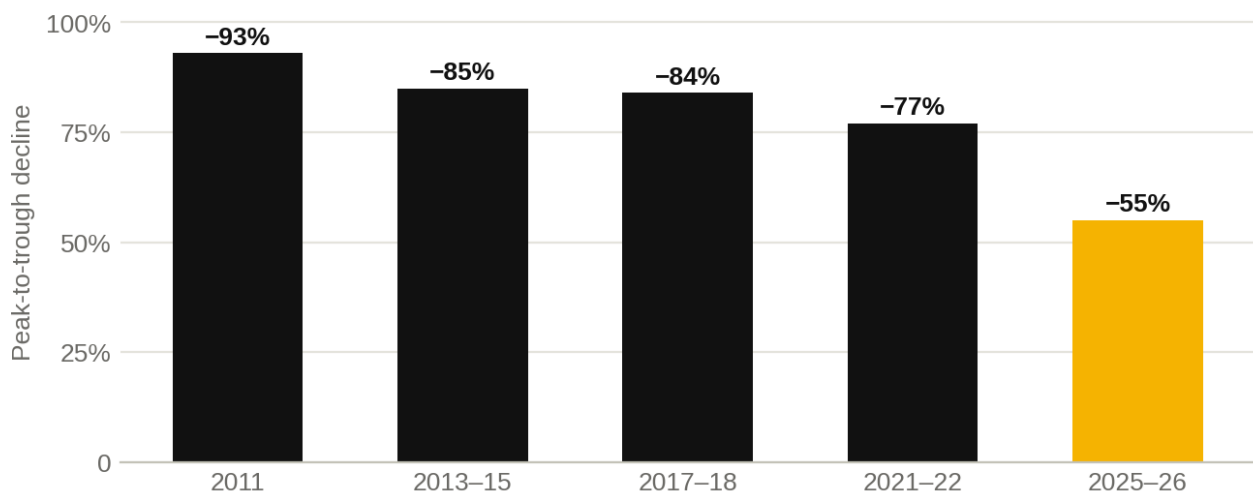
The record

Bitcoin has lost more than 75% of its value four separate times — in 2011, 2014, 2018, and 2022. Each time, the people who'd declared it dead had a decent case. Each time, it recovered to a higher high than before. It traded under a dollar in 2010, crossed \$1,000 in 2013, \$20,000 in 2017, and \$100,000 in 2024, with a high around \$126,000 in October 2025. It then fell more than half, to under \$60,000 by early summer 2026, and has since climbed back into the \$80,000s. Anyone who tells you this is a smooth ride is selling something.

Zoom out, though, and there's a pattern. The swings are enormous but the floor keeps rising. Bitcoin has never traded below its prior cycle's high for long. And the size of each drawdown, in percentage terms, has been getting smaller — 93%, then 85%, then 84%, then 77%, then the roughly 55% of the latest cycle — as the pool of holders gets bigger and more patient.

What the volatility is

Four crashes of 75% or more, each shallower than the last



Approximate peak-to-trough declines by cycle. 2025–26 reflects the drawdown to early summer 2026.

Here's the framing that makes it make sense. Bitcoin isn't a mature money that's oddly unstable. It's an asset in the process of *becoming* money — being adopted, one holder at a time, by a world that hasn't decided yet how much of it it wants. The price is the market's running estimate of the answer to a very big question: how much of the world's savings will eventually sit in the only asset with a fixed supply?

That estimate gets revised constantly, and every revision moves the price. When a country adds it to reserves, when an ETF launches, when a large company puts it on its balance sheet, when a regulator turns friendly or hostile, when interest rates rise and cheap money dries up — each of these is new information about the size of the eventual market, and a fixed-supply asset has no choice but to reprice. Gold went through something similar, in slower motion, over centuries. Bitcoin is doing it in decades, in public, with a price ticker.

The cycles have a rhythm, and it isn't mysterious. A halving cuts new supply. Price rises. Attention follows price, and new buyers arrive who've never seen a drawdown. Leverage builds. Something breaks — an exchange, a fund, a macro shock — and the leveraged buyers are forced out. Price falls until only the patient are left. Then the next halving comes. Every cycle, the base of patient holders is larger, and the top and bottom are both higher than the last. This is what monetization looks like from the inside.

Reading it without losing your mind

Two things help. The first is time frame. Over any one-month window, Bitcoin is a coin flip. Over any four-year window — long enough to include a full cycle — it has never been below where it started. That's not a guarantee about the future; it's a description of what "volatile with a rising floor" means in practice, and it's why the people who've done well are overwhelmingly the ones who bought and waited, not the ones who traded.

The second is that the blockchain is public, which means you can see what holders are actually doing rather than guessing from the price. When long-term holders are accumulating through a drawdown, that's visible. When new buyers are chasing a rally at prices where earlier buyers finally broke even — as happened in September 2026, when Bitcoin stalled at the level where a million coins had been bought the year before — that's visible too. The on-chain tools that make this possible are what the Bitcoin Bites series is about, and they're the closest thing there is to seeing the market's mind.

The part that surprised people in 2026

There's one more thing worth saying about volatility, because it changed this year. For most of its life, Bitcoin traded like a technology stock with extra risk — up when markets were euphoric, down harder when they weren't. In the fall of 2026 that started to break. The Federal Reserve raised rates for the first time in three years, the 10-year Treasury yield climbed past 5% for the first time since 2007, and the dollar rallied. On the textbook reading, every one of those should have hurt Bitcoin. Instead it rose through all of them, absorbed billions of dollars of ETF inflows, and finished its second-best third quarter on record.

That doesn't prove anything on its own. But it's the first extended stretch in which Bitcoin behaved less like a bet on risk appetite and more like a bet on the monetary system itself — which is the thing it was designed to be. The next chapter is about why that connection exists.

What to remember: Bitcoin has lost three-quarters of its value four times and made a new high after each. That's not instability in a finished money; it's the price of an asset being adopted as money, in real time, with every new piece of information repricing a fixed supply. The drawdowns are shrinking as the holder base grows, and in 2026 it began, for the first time, to trade on the monetary story rather than the risk-appetite one.

CHAPTER 7

Bitcoin and the bond market

This is the chapter BOLT exists for. Most introductions to Bitcoin stop at "it's scarce and nobody controls it." That's true, and it's not enough. Scarce things sit at a stable price for decades if nobody needs them. The question that matters is *why anyone would need this one* — and the answer runs through the U.S. Treasury market, which is the largest, most important, and most quietly stressed market in the world.

The system underneath everything

When a government spends more than it collects, it borrows by selling bonds. U.S. Treasury bonds are the foundation of the global financial system: banks hold them as reserves, pension funds hold them as the "safe" part of a portfolio, foreign central banks hold them as the backing for their own currencies, and the interest rate on them sets the floor for the cost of every other loan on earth. The 10-year Treasury yield is, in a real sense, the price of money.

For decades this worked because the numbers were manageable. Debt was a fraction of the economy, interest rates could rise and fall without breaking anything, and the rest of the world wanted to hold dollars and was happy to lend them back. Three things have changed.

The debt is bigger than the economy. U.S. federal debt is now around 120% of GDP, a level last seen at the end of World War II — except then the country had just won a war and was about to grow for thirty years, and now it's running peacetime deficits above 6% of GDP with no plan to stop.

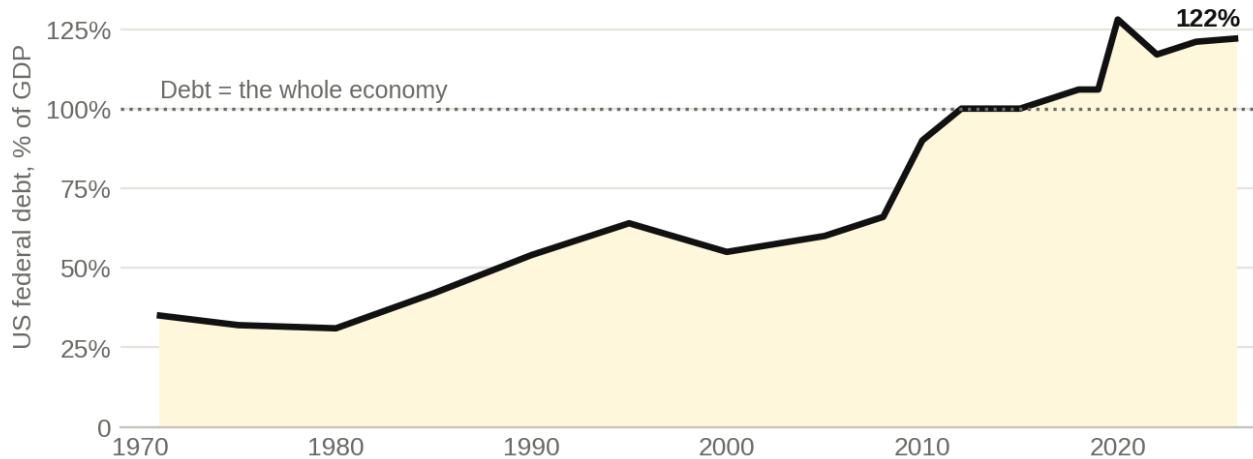
Interest is eating the budget. When rates were near zero, the debt was almost free to carry. Now, with the 10-year above 5%, net interest payments are projected to reach more than 4% of GDP — more than the entire defense budget. Every rate increase makes it worse, which puts the Federal Reserve in a bind it has never faced: raising rates to fight inflation now directly widens the deficit that causes inflation.

The foreign buyers are leaving. For most of this century, the rest of the world funded U.S. deficits by buying Treasuries. That has reversed. Foreign official holdings have fallen, China's are at their lowest

since 2008, and the marginal buyer of U.S. debt is now the domestic financial system — hedge funds, banks, and increasingly, in one form or another, the Fed itself. When a country's own institutions become the main buyer of its own debt, the debt is being funded by money creation, whether or not anyone calls it that.

Why trust is the whole game

Debt past the size of the economy — a level last seen after WWII



Source: US Treasury, BEA (FRED GFDEGDQ188S). Values approximate, as of September 2026.

A bond is a promise: give me your money now and I'll give you more later. The promise is only worth what the promiser's word is worth, and the U.S. government's word has been, for a century, the best in the world. But "best in the world" is measured against alternatives, and the alternatives are being tested.

In 2022, the United States froze the dollar reserves of the Russian central bank — hundreds of billions of dollars that Russia had held in the belief that Treasuries were neutral. Whatever you think of the decision, every other government noticed: dollars you hold at the pleasure of the U.S. Treasury are not entirely yours. In 2026 the same tool was pointed at Iran's airlines, at anyone who fueled them, and — through a proposed ban on diesel exports — implicitly at allies like Japan. Each use of the dollar as a weapon is rational on its own terms. Each also gives the rest of the world a reason to hold something else.

They have. Central banks have been the largest buyers of gold in decades. China imported a record \$159 billion of gold in the first eight months of 2026 alone, and it's building the plumbing in Hong Kong to settle trade in it. The world isn't abandoning the dollar; it's stopped adding to its dollar reserves and started diversifying into assets that can't be frozen, printed, or sanctioned. Gold is the oldest of those. Bitcoin is the newest.

Where Bitcoin fits

Put the pieces together. The reserve asset of the world is issued by a government that can't stop borrowing, is increasingly funded by its own money creation, and has shown it will freeze the holdings of anyone it disagrees with. The traditional escape hatch, gold, is being bought aggressively — but gold is slow to move, hard to verify, and, as history shows, easy for governments to confiscate or overstate.

Bitcoin is the first asset that has gold's properties — fixed supply, no issuer, no counterparty — plus properties gold doesn't have: it can be sent anywhere in minutes, it can be verified by anyone, and it can be held in a way that no one can seize without your cooperation. For a person or an institution or a country asking "where do I keep value that no one else controls," it is a new answer to a very old question.

That's why the connection between Bitcoin and the bond market matters, and why BOLT tracks yields, the dollar, and gold every week alongside the Bitcoin price. When trust in the system erodes — when yields rise on a rate hike instead of falling, when foreign buyers step back, when the dollar gets weaponized — the assets that don't require trust get bid. Bitcoin's 2026 behavior, rising through a hawkish Fed and 5% Treasuries, is what that looks like when it starts to happen. It isn't a prediction. It's a description of the mechanism, and the mechanism is running.

What to remember: Treasuries are the foundation of the global financial system, and that foundation is under more strain than at any point in modern history: debt above GDP, interest costs above defense, foreign buyers retreating, and the dollar increasingly used as a weapon. Every one of those pushes the world toward assets no government controls. Gold is the old answer; Bitcoin is the new one, and it's the reason BOLT reads the bond market every week.

The energy question

"Bitcoin uses as much electricity as a mid-sized country." You've heard some version of this, and it's roughly true — estimates put the network's consumption in the range of 150 to 200 terawatt-hours a year, comparable to Poland or Argentina. The question is whether that's a scandal or a feature, and the answer depends on understanding what the electricity buys and where it comes from.

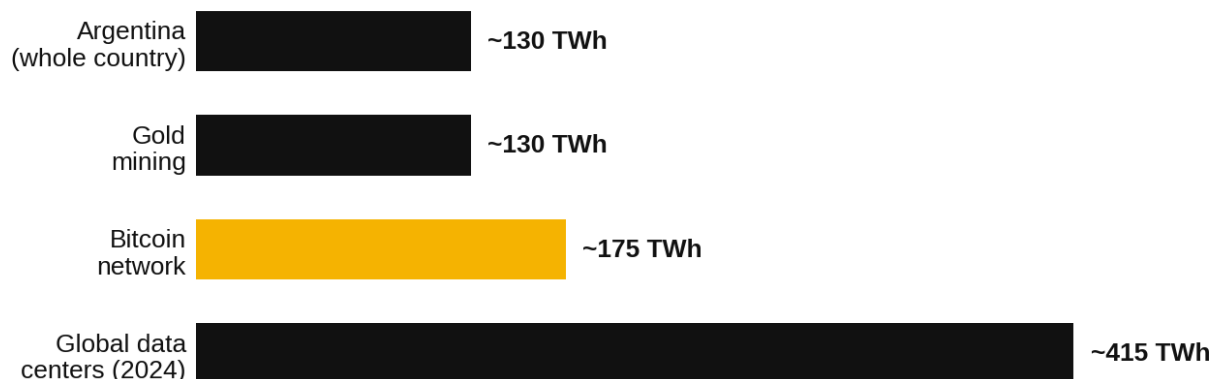
What the energy is for

Chapter 3 covered the mechanism: miners spend electricity on a guessing game, and the cost of that game is what makes Bitcoin's history impossible to rewrite. That's not a side effect. It is the security model. A ledger that costs nothing to write costs nothing to forge. Every other approach to digital money puts a trusted institution in the middle; Bitcoin replaces the institution with a cost that no attacker can afford to pay.

So the right comparison isn't "Bitcoin vs. a database." It's "Bitcoin vs. the system it replaces." The global banking system — its buildings, its data centers, its armored trucks, its hundreds of thousands of branches, the gold vaults underneath — consumes far more energy than Bitcoin does, and nobody frames that as a scandal because the cost is spread across a million invisible line items. Bitcoin's cost is visible, measurable, and concentrated, which makes it an easy target and, oddly, an honest one.

Where miners go

About a mid-sized country, and well under the data centers



Annual electricity use, terawatt-hours. Sources: Cambridge CBEI, IEA, World Gold Council estimates. Approximate.

Here's the part that surprises people. Miners have exactly one input cost that matters — electricity — and they compete on it ruthlessly. A miner paying 8 cents a kilowatt-hour loses to a miner paying 4 cents. So miners go wherever power is cheapest, and power is cheapest where nobody else wants it: next to a hydro dam in a remote valley, at a gas well that would otherwise flare its excess into the atmosphere, in a wind field at 3 a.m. when demand is nil and the turbines would otherwise be curtailed.

This is stranded energy, and the world has a lot of it. Roughly a third of Bitcoin's power comes from sources that would otherwise be wasted, and the overall mix is more than half from renewable or nuclear sources — a higher share than the U.S. grid as a whole. Not because miners are environmentalists, but because clean energy in the wrong place is cheap energy, and miners are the only customer who can show up anywhere with a shipping container and start buying.

Mining also does something no other electricity customer does: it can switch off instantly. When a Texas heat wave pushes the grid to its limit, miners power down within seconds and sell their capacity back, which is why the state's grid operator has come to treat them as a stabilizing resource rather than a burden. A factory can't do that. A data center running an AI model can't do that. A miner can, and gets paid for it.

The comparison that matters now

In 2026 the energy conversation has a new reference point, and it's worth being precise about. The buildout of AI data centers is, by every estimate, the largest new source of electricity demand in a generation. Morgan Stanley projects data-center demand of 257 gigawatts in the U.S. by 2028, against a supply gap of 30 to 40 percent — a shortfall of roughly six New York Cities' worth of baseload power. That demand is inflexible: a data center serving a model to millions of users can't switch off when the grid gets tight, and it wants to sit near cities, on the same lines that homes and hospitals use.

Bitcoin mining is the opposite on every axis. It's flexible, it's location-agnostic, and it goes to the power nobody else wants. The two are often lumped together as "energy-hungry computing," and the lumping is a mistake. One is a new, rigid load competing with everything else on the grid. The other is a buyer of last resort that makes marginal power projects viable and turns off the moment someone else needs the electrons.

None of this makes Bitcoin's energy use free. It's a real cost, paid in the real world, and the honest position is that it buys something — a monetary system without a trusted party — that you either think is worth it or don't. What it isn't is waste, in the sense of energy that could have been used for something else. Most of it couldn't.

One more thing

The energy debate usually assumes electricity is the scarce thing and Bitcoin is spending it. Turn that around. In a world where AI is going to want every watt it can find, where the grid is twenty years behind on generation, and where the price of a transformer matters more than the price of a chip, the interesting question is what money looks like when the physical constraint is energy. A money whose supply is fixed and whose creation is tied directly to real-world power is a strange fit for the 20th century's assumptions and a natural fit for the 21st's. That's a bigger argument than this guide can make. But it's the one your authors spend their day jobs on, and it's coming up in the newsletter more every month.

What to remember: Bitcoin's electricity use is real, visible, and the source of its security — a ledger that costs nothing to write costs nothing to forge. Miners chase the cheapest power, which means stranded, remote, and off-peak energy that would otherwise be wasted, and they can switch off instantly when the grid needs it. That makes them the opposite of the AI data-center load now straining the grid, even though the two get lumped together.

CHAPTER 9

Holding it

Everything so far has been about what Bitcoin is. This chapter is about what it means to have some, because the answer is different from anything you've owned before, and the difference trips people up.

There is no account

When you have dollars at a bank, the bank has your dollars and a record that they're yours. When you have bitcoin, nobody has it. There are coins recorded on the ledger as belonging to a certain key, and whoever controls that key controls the coins. That's it. No name, no account number, no institution that can look you up and confirm they're yours. Chapter 3 put it as "the key is the ownership," and that's literal.

The key is a **private key**: a random number so large that guessing it is impossible in any meaningful sense (there are more possible keys than atoms in the observable universe). Because a 78-digit number is impractical to write down, wallet software translates it into a **seed phrase** — 12 or 24 ordinary English words, in a specific order, from which the key can be reconstructed. Those words *are* your bitcoin. Anyone who has them has your coins; if you lose them, no one can help you. There is no "forgot password" link, because there is no company on the other end.

This is the trade. Bitcoin gives you money no one can freeze, seize, or dilute — and in exchange, no one can rescue you either. For a lot of people that's the first time in their lives they've held something whose safety is entirely their own responsibility. It's worth sitting with before deciding how you want to handle it.

Two ways to hold it

Custodial. You buy bitcoin through an exchange or an app, and it stays there. The company holds the keys; you have a login. This is how most people start, and it's the right choice for many — it's familiar, it's convenient, and if you forget your password there's a reset button. The cost is that you've reintroduced the middleman Bitcoin was built to remove. The company can be hacked (several large ones have been), can go bankrupt with customer funds inside (several have), can freeze your withdrawals, or can be ordered to. "Not your keys, not your coins" is repeated in Bitcoin circles not as a slogan but as a warning that has been proven expensive many times.

Self-custody. You hold the keys yourself, usually on a small device called a hardware wallet — a purpose-built gadget that keeps the private key offline and signs transactions without ever exposing it to your computer or phone. You write the seed phrase on paper or stamp it into metal, store it somewhere safe, and the bitcoin is yours in the fullest sense: no company, no permission, no counterparty. The cost is responsibility. Lose the phrase and the device, and it's gone. Let someone photograph the phrase, and it's theirs.

There's no universally right answer, and plenty of people do both — an exchange balance for convenience, cold storage for the long-term holding. The reasonable rule of thumb most of the community lands on: keep on an exchange only what you'd be comfortable losing if the exchange disappeared tomorrow, and move the rest.

Getting the seed phrase right

If you do self-custody, almost every catastrophe comes from the seed phrase, so here's the short list that covers most of them.

Write it down physically, never in a photo, a note app, an email, or a cloud drive — anything that can be searched or synced can be stolen. Store it somewhere that survives fire and water; metal backup plates exist for this reason. Consider keeping a second copy in a second location. Never type it into a website, and treat anyone who asks for it — including anyone claiming to be "support" — as a thief, because they are. And before you move any serious amount to a new wallet, test the recovery: wipe the device, restore from the phrase, confirm the same addresses come back. Do it once, with a small amount, and you'll never wonder whether your backup works.

Where did the randomness in that seed phrase come from? It matters, and there's a Bitcoin Bite on exactly that question. The short version: use a reputable hardware wallet, and let it generate the phrase rather than choosing your own words.

What you're actually holding

One last reframe. The coins never leave the blockchain. What you hold — in an exchange login or on a hardware wallet — is the ability to sign the next transaction that moves them. That's why the same bitcoin can be held in a way that a government could seize in an afternoon or in a way that no one on earth could take without your cooperation. The asset is identical. The difference is entirely in how the key is kept, and it's the one decision about Bitcoin that's fully in your hands.

What to remember: Owning bitcoin means controlling a private key, expressed as a 12- or 24-word seed phrase; there is no account and no reset. Leaving coins on an exchange is convenient and reintroduces the middleman; holding your own keys is sovereign and makes you responsible. Whichever you choose, the seed phrase is the whole game — write it down physically, store it safely, never share it, and test the backup.

How to keep learning

You now know more about Bitcoin than most people who have opinions about it. You know what money is for and why the current version does the job badly. You know the problem Bitcoin solved and, roughly, how. You know why 21 million holds, who's in charge (nobody), why the price does what it does, how it ties to the bond market and the grid, and what it means to hold it. That's the foundation. Here's how to build on it.

Learn to read the chain

Bitcoin's ledger is public, which means it's the first financial market in history where you can watch the participants instead of guessing at them. A whole discipline — on-chain analysis — has grown up around this, and its tools answer questions no stock market can: Are long-term holders selling or accumulating? Are the coins moving old or new? What did the average holder pay? Is the market in profit or underwater?

None of it is complicated once someone explains it plainly, and that's what the Bitcoin Bites series does — one tool a week, no jargon, tied to what's happening that week. The first eighteen are collected in *The Bitcoin Bites Collection*, which you can get free with a subscription. If this guide was the "why," that one is the "how to see it."

Questions worth asking

As you read more, most of what you'll encounter is either hype or fear, and a handful of questions cut through both.

Who benefits if I believe this? Someone selling a token, a course, or a trading signal has a reason to make Bitcoin sound simpler or more urgent than it is. Someone whose institution is threatened by it has a reason to make it sound sillier or more dangerous. Neither is a reliable narrator.

Is this a claim about Bitcoin, or about a company? Exchanges fail. Funds blow up. Scams use the word "crypto." Bitcoin, the network, has run without interruption since 2009. Most bad headlines are about the businesses around it, not the thing itself.

What does the chain say? Price is what people are willing to pay right now. The ledger shows what they're actually doing. When the two disagree, the ledger is usually ahead.

What's the time frame? Nearly every confident statement about Bitcoin is true on one horizon and false on another. Over a month it's a coin flip. Over a cycle it has never lost. Know which one you're being asked about.

Where BOLT fits

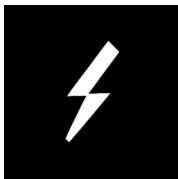
The Weekly BOLT is a free email, every Monday, that connects the three things this guide has been about: what's happening in Bitcoin, what's happening in the bond market and the dollar, and what's happening in energy and the real economy that ties them together. It's written for people who want to understand what's going on without reading forty headlines — the market data, the week's story, the geopolitics, and one Bitcoin Bite, in a form you can read over coffee.

It is not investment advice, and it will never tell you what to buy. It will tell you what happened, what the numbers were, and what the mechanism underneath looks like, and then trust you to think for yourself. That's the whole idea.

Subscribe at **staybolted.com**. Read the archive and the Bites at **staybolted.com/learn**. And if this guide saved you an hour of confusion, there's a Lightning address at **staybolted.com/tip** — value for value, the way it's supposed to work.

Stay Bolted.

What to remember: The next step is learning to read the chain, which is what the Bitcoin Bites are for. When you read about Bitcoin, ask who benefits, whether the claim is about the network or a company, what the ledger says, and over what time frame. BOLT is the Monday email that does that work for you — free, factual, and never advice.



Bitcoin, Explained is published by Stay Bolted, LLC for informational and educational purposes only. It is not financial, investment, legal, or tax advice. Figures are approximate and current as of September 2026. Bitcoin involves significant risk, including potential loss of principal. Do your own research.

Stay Bolted — BOLT Team
staybolted.com