FUNDAMENTALS

Bitcoin: Why It Exists

Before asking 'should I buy Bitcoin?', ask the better question: what problem does it solve? A first-principles exploration of digital scarcity, trust, and why 21 million matters.

James
Chief Strategist

12 min

Most explanations of Bitcoin start with technology: blockchain, cryptography, mining. This is backwards. Technology is the how. The interesting question — the one that actually matters — is why. What problem was so important that someone spent years building an entirely new form of money to solve it?

The Problem Nobody Knew They Had

Imagine you could email gold. Not a picture of gold, not a certificate representing gold, but actual gold — instantly, anywhere, to anyone, without asking permission from a bank, a government, or any intermediary.

This was impossible until 2009. Not because we lacked the technology to move digital files — we'd been doing that for decades. The problem was deeper: digital things can be copied infinitely. Your holiday photo, your Word document, your music file — they can exist in unlimited copies simultaneously. That's a feature when you're sharing memories. It's a fatal flaw when you're trying to create money.

Money requires scarcity. If you could copy a £100 note as easily as copying a JPEG, the economy would collapse within hours. So for decades, digital "money" required a trusted gatekeeper — a bank, a payment processor, a government — to maintain a

ledger and prevent double-spending. You didn't really send money; you asked permission from institutions to update their records.

This worked well enough in stable economies with trustworthy institutions. But it created a dependency that most people never questioned — until they had reason to.

> *"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust." — Satoshi Nakamoto, 2009*

When Trust Breaks Down

For those of us in stable economies, the idea that money could simply stop working feels abstract. But it happens more often than comfortable people like to admit:

- In 2013, Cyprus confiscated up to 47.5% of bank deposits above €100,000 during its financial crisis — money people believed was safely "theirs"
- In 2016, India's government invalidated 86% of its currency overnight, with four hours' notice, affecting 1.3 billion people
- In 2023, Lebanese banks had been refusing withdrawals for three years while the currency lost 98% of its value — savings accounts became fiction
- In 2022, Ukrainian refugees fled with nothing but phones — those who held Bitcoin could access their wealth across any border

These aren't hypotheticals. They're recent history. And they share a common thread: people who trusted institutions discovered that trust could be revoked without warning.

KEY INSIGHT

Bitcoin didn't set out to replace your bank account. It set out to create a form of money that works even when institutions don't — money that requires no trust because the rules are enforced by mathematics rather than policy.

How It Actually Works

Bitcoin solved the digital scarcity problem through an elegant insight: instead of trusting one institution to maintain the ledger, let thousands of computers maintain identical copies. If they all agree on the same transaction history, and any tampering would be immediately visible to all, you've created truth without trust.

Think of it like this: imagine a town square with a giant whiteboard visible to everyone. Every transaction is written on the board. Anyone can propose a new transaction, but it only becomes "real" when the majority of observers confirm it matches their own records. Cheating isn't just difficult — it's publicly visible.

This is the *blockchain* : a shared, public record that everyone can verify and no one can alter retroactively. Every ten minutes, new transactions are bundled into a "block" and added to the chain. Each block references the one before it, creating an unbroken history back to the very first transaction in 2009.

The "miners" you've heard about aren't digging for coins — they're competing to validate transactions and add new blocks. This competition requires significant computational work, which serves two purposes: it makes the system expensive to attack, and it creates a fair way to distribute new Bitcoin into circulation.

Why 21 Million Matters

Here's where Bitcoin diverges most dramatically from the money you're used to: there will only ever be 21 million Bitcoin. Not because someone promised. Not because of policy. Because of mathematics.

The issuance schedule is written into Bitcoin's code, verified by thousands of computers worldwide. The last Bitcoin will be mined around the year 2140. No government, no corporation, no charismatic leader can change this. Attempting to do so would create a fork — a separate network that the rest of the world would simply ignore.

Compare this to traditional currency. Since 2020, roughly 40% of all US dollars in existence were created. The Federal Reserve can — and does — create new money whenever it deems necessary. Whether this is good policy is genuinely debatable. What's beyond debate: each time it happens, the dollars you hold become worth slightly less.

> *"Gold is scarce because nature made it so. Bitcoin is scarce because mathematics made it so. Both are hard to find; only one can be sent across the world in ten minutes."*

This fixed supply is why institutions increasingly frame Bitcoin as "digital gold" — a scarce asset that can't be diluted by policy decisions.

What Bitcoin Is Not

Honest analysis requires acknowledging limitations. Bitcoin is not trying to do everything, and it's not good at everything:

It's not a payment system for coffee. Bitcoin processes roughly 7 transactions per second. Visa handles 65,000. This isn't a bug being fixed — it's a deliberate trade-off for decentralisation and security. Solutions like the Lightning Network address this for small payments, but Bitcoin's base layer is designed for settlement, not retail transactions.

It's not anonymous. Every transaction is publicly visible forever. It's pseudonymous — your name isn't attached, but sophisticated analysis can often trace activity. If privacy is your primary concern, Bitcoin is likely the wrong tool.

It's not stable. Bitcoin has dropped 80% or more multiple times in its history. If you need your money to have the same value next month, Bitcoin is unsuitable. Its volatility is a feature for speculators and a serious drawback for most practical uses.

It's not without environmental cost. Bitcoin mining consumes significant electricity — roughly comparable to a small country. Whether this is justified depends on how much value you place on what Bitcoin provides. The same argument applies to gold mining, air conditioning, or Christmas lights. It's a values question, not a technical one.

The Investment Lens

From an institutional perspective, Bitcoin has evolved from curiosity to asset class. BlackRock, Fidelity, and other major asset managers now offer Bitcoin ETFs. This isn't endorsement of ideology — it's recognition of demand and, arguably, legitimacy.

The bull case: In a world of expanding money supplies, unprecedented government debt, and increasing geopolitical uncertainty, a provably scarce, globally accessible asset has a logical place in portfolios. Even a 1-3% allocation provides meaningful upside exposure with limited impact if the thesis fails.

The bear case: Bitcoin produces no cash flows, pays no dividends, and has no intrinsic value beyond what the next buyer will pay. It's entirely possible that a better technology emerges, that governments crack down effectively, or that institutional interest proves temporary. The 80%+ drawdowns aren't anomalies — they're part of the historical pattern.

> **THE RORY SUTHERLAND TAKE**
>
> Bitcoin's real innovation isn't speed or cost — traditional finance is often faster and cheaper. The innovation is optionality without permission . You don't need anyone's approval to hold it, move it, or use it. In a world of increasing financial surveillance and capital controls, that option has value — even if you never exercise it. You're not paying for what Bitcoin does today. You're paying for what it could do if you needed it.

The rational approach: Understand what Bitcoin is. Decide whether it fits your objectives and worldview. Size any position according to your risk tolerance — small enough that an 80% drop wouldn't cause financial distress, large enough that meaningful appreciation would matter. And don't check the price daily. That way lies madness.

When In Doubt, Zoom Out

Bitcoin was worth nothing in 2009, $1 in 2011, $1,000 in 2013, $20,000 in 2017, $3,000 in 2018, $69,000 in 2021, $16,000 in 2022, and over $100,000 in 2024.

Every crash felt like the end. Every recovery seemed impossible. The obituaries number in the hundreds. Yet here we are — fifteen years later, with Bitcoin still functioning exactly as designed, processing transactions every ten minutes, never successfully attacked, never shut down, now held by the world's largest asset managers.

The question isn't whether Bitcoin is volatile. It is. The question is whether the underlying technology and thesis remain sound. After fifteen years and countless attempts to break it, the answer appears to be yes.

Whether that matters to you — whether the problem Bitcoin solves is a problem you have — is a different question entirely. And that's one only you can answer.

S.

Our secret. Your edge.

Discover more at sirruna.com