Bitcoin, Austrian Economics, and the Regression Theorem

What Is Mises' Regression Theorem?

Ludwig von Mises, one of the most important economists of the Austrian School, faced a problem: explaining money's value seemed circular. Money has purchasing power because people demand it, but people demand it because it has purchasing power. His solution, the regression theorem, broke this circle by introducing time.

People value money today based on what it could buy yesterday. Yesterday's value was based on the day before. You can trace this chain backwards through history until you arrive at the moment when the good was first valued — not as money, but for some other reason entirely. That original, non-monetary demand is what anchors the whole chain.

Mises also described how money evolves. First, a good must be valued by someone for any reason. Then people begin acquiring it not to consume it, but to trade it later for something else. At that point it becomes a **medium of exchange**. If one medium of exchange outcompetes all others and becomes dominant — the thing most people in an economy reach for when they need to transact — it becomes **money**.

These are two distinct categories. All money is a medium of exchange, but not all media of exchange are money. Lots of things throughout history have served as media of exchange — cattle, salt, shells, silver, tobacco. Money is the one that wins.

What Gave Gold Its Value?

Gold is the textbook example of Mises' framework in action. But it's worth examining *why* gold was valued in the first place.

Gold was prized for ornamentation — jewelry, decoration, symbols of status. But why? Not simply because it was pretty. Copper is pretty. Pyrite is shiny. Gold was prized because it was **scarce**, because it **didn't tarnish** (durability), and because it **couldn't be easily faked** (forgery resistance). The ornamental value was downstream of these properties. A king wearing a gold crown was signalling wealth precisely because gold was hard to obtain. If gold were as common as sand, nobody would have cared about gold jewelry.

So the regression chain for gold looks like this: scarcity and durability → desirability as ornament → commodity value → medium of exchange → money.

Scarcity sits at the very base.

Where Does "Store of Value" Fit?

"Store of value" is not a formal stage in Mises' original framework. His theory deals with medium of exchange and money. Storing value is implicit in holding any medium of exchange — you receive it, hold it for some time, then spend it. During that holding period, it's storing value by default.

The sequence that is commonly used in Bitcoin discussions — store of value → medium of exchange → unit of account → money — was built around Mises' theory by the Bitcoin community. It's a useful way to describe Bitcoin's monetisation path, but it extends Mises rather than restating him.

The logic behind this extended sequence is: people first store value in something because they trust its properties (scarcity, durability, forgery resistance). Because enough people store value in it, it becomes liquid. Because it's liquid, people start accepting it in exchange for goods — now it's a medium of exchange. Once it's so widely used that people start pricing things in it and thinking in it natively, it becomes a unit of account. At that final stage, it's money.

Does Bitcoin Satisfy the Regression Theorem?

This is one of the most debated questions in Austrian economics. Bitcoin appears to have no commodity use — you can't wear it, eat it, or build with it. At first glance, this seems to violate the regression theorem's requirement that a medium of exchange must trace back to some original non-monetary demand.

But Bitcoin is empirically a medium of exchange today. People buy it, hold it, and trade it for goods and services. That is not debatable. Within Mises' own framework, this means the regression theorem *must* apply to it — the chain must be anchored somewhere, even if identifying the exact anchor is difficult.

Several plausible anchors have been proposed:

- **Entrepreneurial foresight** (Daniel Krawisz) — early adopters recognised Bitcoin's potential to become money and acquired it on that bet, just as an entrepreneur might stockpile a newly discovered resource before the rest of the world catches on
- **Technological utility** (Peter Šurda) — the ability to transfer value without intermediaries, across borders, without permission, was itself a useful non-monetary function
- **Engineering appreciation** (Konrad Graf) — cryptographers and developers valued Bitcoin as an elegant, novel system worth engaging with; geek appeal, curiosity, and the challenge of participating in something new
- **Collectors' impulse** (Satoshi Nakamoto) — Satoshi himself suggested that collectors or "any random reason" could spark initial value, just as humans have always instinctively collected scarce objects
- **Proto-money collectible behaviour** (Nick Szabo) — archaeological evidence shows humans were collecting scarce, hard-to-forge shell beads 75,000 years ago, long before anything we'd call commerce existed; Bitcoin follows the same instinct
- **The theorem doesn't apply** (Laura Davidson & Walter Block) — Bitcoin emerged within an existing price system with dollars, euros, and established markets, not from pure barter; the regression theorem was designed for the barter-to-money transition and is simply irrelevant here
- **Pure subjective valuation** (George Pickering) — the theorem only requires that *somebody* valued it before the first exchange, for *any* subjective reason; it doesn't require economists to understand or approve of that reason

- **Ideological utility** (cypherpunk thesis) — Bitcoin was valued as a working proof of concept that money could exist outside state control, a tool of political resistance against financial surveillance
- **The subjectivist critique** — if subjective value theory is a pillar of Austrian economics (value exists only in the mind of the individual), then it's internally contradictory to claim something *cannot possibly* be valued first as a medium of exchange
- **Proof-of-work energy expenditure** — mining bitcoin requires the irreversible consumption of real electricity; this injected real-world cost into every bitcoin from day one, and the first known exchange rate was explicitly calculated from this energy cost

These explanations are not mutually exclusive. Several were likely true simultaneously for different early participants. The regression chain doesn't require a single explanation — it requires that enough people valued bitcoin for any reason before the first exchange. And they did.

The Energy Bootstrap

Among the possible anchors, the energy argument deserves particular attention because it grounds Bitcoin's value in physical reality.

To mine bitcoin, real electricity — real energy — must be consumed. That energy is used to solve cryptographic puzzles rooted in mathematics. Energy and mathematics are as concrete a foundation as we have currently discovered — two pillars of reality that don't depend on human institutions, opinions, or promises. Bitcoin's system is anchored in both.

But the deeper insight is *why* energy specifically, and this gets to what may be the most important technical idea in the entire system.

How Do You Tie a Digital Artifact to the Physical World?

This is the problem Satoshi had to solve, and it's a problem that had never been solved before. Digital things are just data — lists of numbers in a computer. How do you make a digital object *real* in the sense that it can't be copied, faked, or conjured out of nothing?

Satoshi recognised that the only real-world asset that can be linked to a computer system in a trustless manner is energy. Nothing else. Every other thing — gold, paper certificates, real estate, strawberries — reintroduces a trusted third party because of the inherent disconnect between the digital and the physical world. Someone must ensure that the real-world assets and their digital representations remain up-to-date and in sync. If you create a digital token that represents a bar of gold in a vault, you still need to trust the person running the vault. You've solved nothing.

This is known as the oracle problem: how does a computer system know that its data reflects reality? It's a variant of Garbage In, Garbage Out — you have to trust whoever is keeping the records that the records are correct. You can never be sure that the data represents reality, *except if the reality is rooted in computation itself.*

Proof-of-work solves the oracle problem in an ingenious, roundabout way: by using energy

— and thus physics — as the base truth. The energy was either spent or it wasn't. That fact is verifiable, irreversible, and doesn't require trusting anyone. No one can fake having spent energy any more than you can fake having run a marathon. The computation *is* the proof, and the proof *is* the value.

This is why proof-of-work is not an arbitrary design choice or a wasteful byproduct. It is the mechanism that ties a digital artifact to the physical world without any intermediary. It is what makes bitcoin *real* in a way no previous digital object had ever been.

The Chain

The result is a chain where each link rests on something that exists independently of human institutions:

Energy (physics) → **cryptographic proof** (mathematics) → **unforgeable costliness** → **verifiable scarcity** (bitcoin) → **exchange value** (price).

Nick Szabo coined the term "unforgeable costliness" to describe the quality that made proto-monies work throughout human history: the cost of production was real, irreversible, and impossible to fake. Proof-of-work is the digital equivalent — the energy was spent, it cannot be unspent, and no one can pretend to have spent it without actually doing so.

The very first known exchange rate for bitcoin (October 2009, roughly 1,309 BTC per dollar) was calculated by dividing the cost of electricity to run a mining computer by the number of bitcoins produced. Bitcoin's first price was literally the cost of the energy required to create it.

The Timeline: How Fast Did This Happen?

- **January 3, 2009** — Satoshi mines the genesis block. Bitcoin exists but has no price. A small group of people mine coins and send them back and forth, testing the system.
- **October 2009** — New Liberty Standard publishes the first exchange rate based on electricity cost. Bitcoin has a price. By Mises' definition, it has become a medium of exchange — something acquired for the purpose of trading it for something else.
- **May 22, 2010** — Laszlo Hanyecz buys two pizzas for 10,000 bitcoin. The first known purchase of a real-world good with bitcoin.

The entire journey from nothing to functioning medium of exchange took roughly nine to sixteen months. For comparison, gold's equivalent journey took centuries or millennia. The speed of this transition is itself notable — by the time anyone was debating whether Bitcoin *could* become a medium of exchange, it already had.

Why Bitcoin Has Value

Bitcoin has value because people wanted it before it was money, and the reasons they wanted it — the real energy burned to create it, the mathematical proof that it can't be faked, and the certainty that there will never be more than 21 million — haven't gone away. They've only strengthened as more people have recognised them.

Bitcoin's monetary properties are worth stating plainly:

- **Scarcity**: 21 million is a hard cap enforced by the protocol. No person, company, or government can change it.
- **Durability**: As long as you keep your cryptographic seed phrase secure, your bitcoin persists regardless of geography, political upheaval, or physical destruction of hardware.
- **Forgery resistance**: It is mathematically impossible to counterfeit a bitcoin or fabricate a transaction. Every transaction is verified by a global decentralised network.
- **Portability**: Bitcoin can be sent anywhere on earth with an internet connection, without permission from any intermediary.
- **Divisibility**: Each bitcoin is divisible to eight decimal places (100 million satoshis), making it usable at any scale.
- **Verifiability**: Anyone can independently verify the entire supply, every transaction, and every rule of the protocol by running a node.

These are not marketing claims. They are properties embedded in the protocol and secured by the largest computational network on earth. They can be audited by anyone, at any time, without trusting any authority.

Where Bitcoin Stands Today in Mises' Framework

Bitcoin has passed the first and hardest hurdle: going from nothing to a functioning medium of exchange. That transition is complete and, after sixteen years of continuous operation, effectively irreversible.

It is now in the middle stage of monetisation. It functions as a store of value for a growing number of people. It functions as a medium of exchange for a smaller but expanding group. It barely functions as a unit of account — almost nobody prices goods natively in bitcoin yet.

Mises described a self-reinforcing feedback loop at this stage: the more marketable a medium of exchange becomes, the more people adopt it; the more people adopt it, the more marketable it gets; less marketable alternatives get squeezed out. This feedback loop is underway. Whether it carries Bitcoin all the way to becoming money in Mises' sense — the dominant medium of exchange — is an open question that the market will answer over time.

How This Is Completely Different From the Greater Fool Theory

A common criticism of Bitcoin is that it's a greater fool scheme: people only buy it because they think they can sell it to someone else for more, and eventually the chain of buyers runs out and the last person is left holding something worthless.

This criticism misunderstands what is actually happening, and it's worth being precise about why.

In a genuine greater fool scenario — tulips, Beanie Babies, speculative tokens with no underlying properties — the chain of buyers is sustained by hype, narrative, and momentum. There is nothing anchoring the value. When the excitement fades, demand disappears and

the price collapses permanently. The asset never recovers because there was never anything underneath the speculation.

Bitcoin does not follow this pattern. The next buyer pays more not because they've been swept up in a story, but because they've independently verified the same properties the previous buyer verified. The scarcity is auditable. The unforgeable costliness is real. The durability is cryptographically guaranteed. The resistance to debasement is embedded in the protocol. None of these properties have changed since the first block was mined, and none of them can be changed without the consensus of the entire network.

The chain of buyers is therefore not a chain of fools finding greater fools. It is a chain of recognition — each new participant arriving at the same conclusion independently, because the properties are objectively verifiable by anyone with a computer and an internet connection. The previous buyer doesn't need to convince the next buyer. The protocol does that.

The empirical evidence confirms this distinction. Greater fool assets crash and stay dead. Bitcoin has experienced multiple drawdowns exceeding 80% and has recovered to new highs every time. That pattern — crash, recover, grow — is not consistent with a speculative mania. It is consistent with volatile monetisation: waves of adoption, overextension, correction, then a new wave arriving with broader understanding.

Where People Get Confused

The confusion between the greater fool theory and Mises' monetisation framework arises because on the surface they can look similar. In both cases, someone buys something expecting to exchange it later. But the underlying logic is fundamentally different.

In the greater fool theory, the expectation of future exchange is *the only thing* sustaining the value. Remove the expectation and the value collapses to zero, because there's nothing else there.

In Mises' framework, the expectation of future exchange is grounded in verifiable properties. People expect bitcoin to be exchangeable in the future because of its scarcity, durability, portability, divisibility, and forgery resistance. These properties don't depend on expectations — they exist whether anyone is looking at them or not. The expectations are a *consequence* of the properties, not a substitute for them.

Another way to see the distinction: ask what happens if sentiment turns sharply negative. In a greater fool scenario, the asset goes to zero and stays there. With Bitcoin, sentiment has turned sharply negative multiple times — exchange collapses, regulatory crackdowns, 80% price drops — and every time, the properties remained intact, new buyers eventually recognised them, and the price recovered. The properties provide a floor that greater fool assets simply don't have.

The "last person holding" in a greater fool scheme is left with something worthless. The last person holding bitcoin is left with a verifiable fraction of a fixed supply, secured by a global network, accessible from anywhere. Those two situations are not comparable.

Summary

Mises' regression theorem says money evolves in stages: original demand → medium of exchange → money. The value chain must be anchored in some original non-monetary demand.

Bitcoin satisfies this framework. Its original demand came from multiple sources — energy cost, technological fascination, ideological conviction, collecting instinct, entrepreneurial foresight. Within sixteen months of its creation it had a price and was being used to buy real goods.

Today Bitcoin is a functioning medium of exchange in the monetisation process. Its properties — absolute scarcity, unforgeable costliness, perfect durability, cryptographic forgery resistance — are not opinions or narratives. They are features of the protocol, verifiable by anyone, unchanged since day one.

Whether Bitcoin completes its journey and becomes money in Mises' full sense is not yet determined. But the question is no longer "can this work?" — that was answered years ago. The question is how far the process goes.