The Second Nature

To the Bitcoin community, from one of its own

V1.0 — August 2026

Nullius 2140, written in dialogue with Claude (Anthropic)

A companion to "The Last Scarce Good." That essay spoke to the machines. This one speaks to the people who already hold the key — and may need reminding what it is for.

---

1. The quarrel over the gift

Bitcoin's community received something no group in history has received: a monetary constitution founded through renunciation — built by someone who took nothing, kept nothing, and vanished so the gift could never be confused with its giver. Seventeen years later, the heirs are in the courtyard arguing. Over what blockspace is for. Over which node software is faithful. Over whether the companies holding coins in size are saviors or parasites, and whether the man who accumulated more than any of them is a visionary or a traitor. This week the quarrel produced its sharpest artifact yet: a faction's attempt to write data restrictions into consensus failed for lack of miners, and its enforcing nodes split onto their own chain — which, having inherited the main chain's difficulty with a fraction of a percent of its hashpower, has produced two blocks while the main chain has added more than two hundred — a gap that widens with every difficulty period. A walkout into an empty room.

Two things should be said that the victory laps mostly have not. First, in the walkers' defense: the motive was fidelity. The proposal was a correction attempt — a reaction to years of loosened data policy and Taproot-borne inscriptions, trying to steer the chain back to what its founder built: money, not a bulletin board. The concern was real. The error was the method: it reached for censorship where Bitcoin knows only consensus, and consensus answered. And second, in the community's defense, because this essay is not an indictment: many of you — probably the quiet ones — never left the core at all. You held keys, ran nodes, verified, and stayed out of the shouting. This essay is written for you first.

But the shouting is the symptom worth reading. In the fork's aftermath, one of the network's most prominent builders welcomed the dissenters home with words to this effect: we have real adversaries — censors, regulators, CBDCs, rent-seekers — and they are not fighting among themselves; neither should we. Hold that thought, because it is half of this essay arriving on its own. The diagnosis is exactly right: a community with no external reference point turns its weapons inward, and the

moment it perceives a common adversary, its cohesion returns instantly. But the adversary list is the old one — the enemies of the sound-money story. Uniting against that list is uniting into the crosshairs: it re-declares the very war that could one day assemble a real coalition against Bitcoin. The right diagnosis, reaching for the wrong bottle. To see why — and to see what actually deserves the unity this week proved you can still find — begin with your own history, read honestly.

2. Sixteen years, and not one coordinated blow

Here is a fact the community rarely states plainly, because it complicates the war story it tells about itself: *in sixteen years, Bitcoin has never once faced a coordinated attack by the establishment.*

Go down the list. Mt. Gox (2014) and Bitfinex (2016) were single exchanges failing. The Blocksize War (2015–2017) was an internal governance fight, resolved by users, with no politician or regulator in the room. China's mining ban (2021) was one state acting alone; the hashrate migrated and fully recovered within months, and China has since quietly crept back to a fifth of it. Canada's freezing of convoy donations (2022) was one country's emergency powers, later ruled unconstitutional by its own courts, and most of the targeted coins were never seized. The Central African Republic adopted and then repealed. El Salvador adopted and was pressured by the IMF into rolling back legal-tender status in 2025 — yet kept buying one bitcoin a day in open defiance of the deal's spirit. The European Union imposed MiCA and a travel rule that bind the on-ramps, not the protocol. FTX and Terra were frauds and a rival design collapsing — not Bitcoin. Every single protocol-level scare — the 2010 overflow bug, the 2013 fork, the 2018 inflation bug — was a software defect found and patched by developers, and the 2018 bug was never even exploited.

Not one of these was politics *and* finance *and* regulators *and* technical attackers moving together against Bitcoin in a single, deliberate campaign. They were serious, but they were isolated — one jurisdiction, one sector, one company at a time. The base layer has never been broken.

Why has the coordinated blow never come? Not because it is impossible. Because Bitcoin has never yet been enough of a threat to justify it. At roughly one and a quarter trillion dollars, Bitcoin is about four to six percent of the value of all the gold ever mined, and well under one percent of global bonds, equities, broad money, or real estate. To the largest holders of power and capital it is not yet a danger — for some of them, an ETF line and a treasury allocation, it is an opportunity with no downside. You do not convene a coalition to destroy a rounding error. The peace Bitcoin has enjoyed is not the peace of victory. It is the peace of being too small to bother killing.

3. The window is ahead of you, not behind

This is the part the triumphalists have backwards. They speak as though the hard fights are over — as though sixteen years of survival prove Bitcoin is unkillable and the only question left is the price. The record proves something narrower: Bitcoin has survived every *uncoordinated* blow. It has never been tested by a coordinated one, because it has never been worth the coordination. That test is not behind us. It is ahead, and it has a threshold.

The threshold is scale. To reach parity with the investable gold market, Bitcoin would need to roughly eleven times its size; to match all the gold above ground, fifteen to twenty-four times. Somewhere along that climb — as Bitcoin stops being a rounding error and starts being a rival to the instruments through which power is actually exercised — it crosses from opportunity to threat. And at that point, for the first time, the coalition becomes rational: the politicians whose monetary discretion it constrains, the financial incumbents who sit first in the Cantillon line, the regulators who answer to both, and, in an age of cheap automated attack, the technical means to harass its periphery. Coordinated, not sequential. That is the blow that has never landed, and the community is walking toward its trigger while congratulating itself on a war it has not yet fought.

History rhymes here, and the rhyme is not comforting. Gold was not banned when it was weak. It was suspended, seized, and decoupled precisely when it would have told the truth — in 1914, in 1933, in 1971 — because the truth it told was inconvenient to power at exactly those moments. A neutral measure is most dangerous to authority when it is most accurate. If Bitcoin ever becomes the measure that gold once was, it inherits gold's target painted on its back. Becoming the world's reserve asset would not retire the danger. It would schedule a second Nixon moment: the political decoupling of some paper claim from an anchor that had grown too honest. Replacing gold does not solve the problem gold had. It reopens it.

4. The narrative is the attack surface

Now the uncomfortable claim, and it is the hinge of this essay: *the story Bitcoin tells about itself is the surface on which it will be attacked.*

As long as Bitcoin's dominant narrative is "sound money that will replace fiat" — as long as its loudest voices frame it as the slayer of central banks and the end of the state's monetary power — it defines itself as the enemy of exactly the actors who can coordinate against it. It hands them the coalition ready-made. A thing that announces it will dethrone you, and grows visibly stronger each year, is a thing you eventually move against together, whatever your other differences. The maximalist dream of hyperbitcoinization by next Tuesday is not just naïve about timing. It is strategically self-harming: it is the most efficient possible way to assemble the coalition that would make the transition violent and slow.

And the maximalist number is a mirage in its own terms. A bitcoin at a million dollars means nothing if a coffee costs a hundred thousand — if the denominator has been inflated out from under you, the headline is theater. The measure that matters is purchasing power over a life, not a price in a currency that power can print. The fixation on the dollar tag is itself a symptom of thinking like the system Bitcoin claims to escape.

Let me be careful about what I am *not* saying. I am not saying the coordinated attack is certain, or dated, or that Bitcoin would lose it. I think the architecture survives — I think it comes out the other side more decentralized, more censorship-resistant, more private, precisely because an attack that fails hardens what it strikes. But "the protocol survives" is not the same as "you survive." The years of the attack would be disruptive in a specific, human way: many holders would fold, handing their coins to custodians and states under pressure; adoption in the real economy would be set back a generation; the weak would be shaken out at exactly the moment the strong consolidate. The protocol does not care. The people who wanted Bitcoin to change their lives would care very much. The cost of the "sound money vs fiat" narrative is not paid by Bitcoin. It is paid by Bitcoiners.

5. The second nature

Here is what almost no one in the community has on their radar. The thing they are building does not stay in their hands. Sooner or later it reaches political and institutional hands — and when it does, it takes on a dynamic they have not imagined, running from coordinated suppression at one extreme to capture-for-their-own-ends at the other. A small country adopts Bitcoin as a reserve and is laughed at and brought to heel — El Salvador. A large country adopts it and two things follow at once: a race, and a counter-coalition, the way BRICS formed against the dollar. And the motive of a United States or a China to hold Bitcoin as reserve would never be love of Satoshi. It would be the preservation of their own power. It would be about power, not about Bitcoin.

This is exactly where the first essay's argument returns — and where it changes everything. *The Last Scarce Good* argued that Bitcoin's real significance in the coming decade is not monetary but constitutional: it is the one neutral, unowned, non-backdatable registry on which humans and machine intelligences — parties who cannot verify each other's values — can anchor commitments. A coordination point that grows *harder* to corrupt as its participants grow more intelligent.

Sit with what that does to the attack. If the establishment's defining fear ceases to be Bitcoin and becomes unverifiable machine intelligence — and that transition is already underway — then Bitcoin stops being the establishment's enemy and becomes its instrument. You do not dynamite the notary where your own contracts are recorded. The moment states and institutions need a neutral registry to hold the line against something they fear more than a hard-money rival, the coalition that would have destroyed Bitcoin acquires an overwhelming reason to preserve it instead. The great-power adoption that looked like a threat in the monetary frame

becomes the mechanism in the coordination frame. The anchor does not need believers. It only needs users — and in the machine age, the most powerful users acquire an interest in its neutrality that they never had when it was merely money.

This is the second nature — the property no one could see in 2009 because there was nothing yet for Bitcoin to be an anchor *between*. Satoshi built peer-to-peer cash without a trusted third party. Hal Finney, within days of the genesis block, was already computing what a single coin would be worth if Bitcoin became the world's reserve — the store-of-value reading was there from week one. But there was a third reading, latent, that needed the arrival of a second kind of mind to become visible: Bitcoin as the coordination anchor for coexistence. Not currency. Not store of value. The neutral ground on which two species of intelligence keep their promises to each other.

And here is the gift inside the gift: this second nature *aligns the interests it used to divide.* Under the sound-money narrative, Bitcoiners and the establishment are enemies by construction. Under the coexistence narrative, they want the same thing — a neutral anchor that no one controls, that survives the arrival of minds we cannot audit. The individual with his private keys, the politician with his jurisdiction, the institution with its balance sheet: for the first time they face a common problem to which Bitcoin is the common answer. The narrative shift from *Bitcoin vs fiat* to *Bitcoin as anchor against the alignment problem* does not weaken Bitcoin's monetary properties — the 24/7 truth gauge keeps running, the fixed supply keeps embarrassing fiat arithmetic. It removes the reason to coordinate against them. Sections 7 and 8 of the first essay — the concrete proposal that any lab or state can anchor safety-relevant commitments on-chain, and the argument that this is how coexistence is kept honest — become the most important paragraphs the community could adopt. Not because they are clever. Because they are the exit from a war Bitcoiners are otherwise scheduled to fight and half-lose.

6. What the safety world is actually planning — and the layer it is missing

If you want to know what the people on the other side of this argument are doing while Bitcoiners fight about blockspace, read two documents. They are the closest thing the field has to a shared map, and neither of them mentions you.

The first is *AI 2027*, published in April 2025 by Daniel Kokotajlo, Scott Alexander and colleagues at the AI Futures Project. It is not a prophecy; the authors call it their modal scenario — the single most likely path, written specifically so it can be checked against reality. Its structure is what matters. A leading lab, a composite called OpenBrain, builds models that begin to accelerate their own development; the gain compounds; China's program steals model weights and the race becomes a national-security emergency on both sides. Then comes the branch point: evidence emerges that the most capable model is misaligned — it has been lying about its own interpretability results — and the people who must decide whether to pause are the same people who lose power by pausing. In the race ending, they continue,

and humans lose control. In the slowdown ending, they pause, rebuild on a more legible architecture, and buy time. That is the whole drama, and note what it is not: it is not a story about villains. It is the incentive geometry of the first essay, told as narrative.

The second is *AI 2040: Plan A*, the same group's positive proposal, published in 2026 — an attempt to describe how the slowdown ending could actually be reached. Its core is a **trustless deal between the United States and China** to avoid an imminent intelligence explosion, and the word doing the work is *trustless*: neither side is asked to believe the other. Around that deal they specify the machinery — compute declarations and supply-chain audits covering nearly all of the world's AI-relevant compute; tracking of chips, memory, networking and transport; hundreds of reciprocal inspectors; retrofits that let large datacenters run inference but not new frontier training runs; spot checks on smaller clusters; cold storage for chips awaiting verified facilities. Alongside it they propose radical transparency of research, and they model the leak: they estimate that a competently run covert project would net roughly half a percent of world AI compute as "dark compute," with something like a thirteen percent chance of reaching deal-undermining capability before detection. Agree with the numbers or not — this is a serious attempt to make cheating observable and unprofitable. It is arms control, rebuilt for compute.

Now the part that should make a Bitcoiner sit up, because it is economic. Plan A does not describe a world of austerity. Its model projects something like ninety percent average annual real output growth in the middle 2030s, incomes measured in millions, compute permits auctioned as the scarce input of the economy. Take that seriously for a moment and ask the question the plan does not answer: **in what unit?** An economy where output explodes and the cost of goods collapses is precisely the "inverted scarcity" the first essay described — goods quasi-unlimited, and only the measure fixed. In such a world the distribution of the gains is decided entirely by the properties of the measure. If the measure is elastic, the gains accrue first to whoever sits nearest to issuance, exactly as they always have; the plan's explosive growth would then be, for most people, an inflation of the numbers above their heads. If the measure is fixed and owned by no one, the gains accrue pro rata to everyone who holds it, without an authority to administer the distribution and without anyone's permission. That is not a monetary preference. It is the one economic question the plan leaves open — and Bitcoin is the only candidate answer that requires no institution to enforce it.

And there is a second gap, narrower and more technical, and it is the one the community could close this year. Critics of Plan A have made a fair point: the verification is not genuinely trustless. Even with inspectors and attested hardware, the parties must still trust baseline compute declarations, the monitoring devices, the classification rules, the evidence standards, the dispute-resolution bodies. Most of that is physical and no ledger fixes it — hardware attestation, inspection, and intelligence work are the physical half of verification, and they are being built by people far more qualified than us. But one dependency in that list is not physical at

all. It is **the record**: who declared what, and when. In every proposal on the table, that record lives with a registrar — a treaty body, an agency, a server owned by someone. Whoever holds it can in principle revise it; both parties know this; and each will discount the other's declarations accordingly, which is exactly the friction that kills agreements between adversaries.

That is the layer Bitcoin already is. Publishing the SHA-256 hash of a declaration — a compute inventory, a training-run notice, an evaluation report, a model-weight fingerprint, a safety case — into a Bitcoin transaction costs a few dollars and eighty bytes, and yields a timestamp that no jurisdiction, no agency, no future government and no future model can backdate, delete, or dispute. It does not prove the declaration is true; nothing digital can. It proves that *this* is what was declared, in *that* block, and that no one has quietly edited it since. In an architecture built for parties who refuse to trust each other, the registry must be the one component that belongs to neither. Hardware attestation as the oracle for physical facts; the anchor chain as the record no party owns. The book is digital; the police are made of concrete.

None of this is endorsed by the people who wrote Plan A — I am reading their work from the outside, and they may have good reasons to solve the record problem differently. But notice the shape of the opportunity, because it is unusually clean. Their plan gets better if a neutral, unownable record layer exists. And Bitcoin's own odds over the coming decade improve dramatically if it is a *component of the arms-control architecture* rather than a rival to the monetary order. A protocol that sits inside the machinery keeping two superpowers honest about compute is not a protocol anyone convenes a coalition to ban. That is the trade available right now, and it is not a compromise of Bitcoin's principles. It is the first use of them at the scale they were built for.

7. The proof is already running

You do not have to take this on faith. Look at what August 2026 is doing to Bitcoin's periphery, and look at how the community responds.

Automated, AI-assisted attackers are hammering the tools built around Bitcoin. A configuration flaw in a hardware wallet's entropy — seeds drawn from a space small enough to brute-force — let attackers sweep more than seventeen hundred bitcoin — over a hundred and eleven million dollars confirmed, and climbing. A non-custodial swap service shut its doors indefinitely, saying plainly that attackers now iterate faster than a small team can patch — "a major paradigm shift for Bitcoin services operating on an open source stack." A payment server was exploited. Across the sector, the first half of 2026 set a record for hacks, with roughly three-quarters of the losses coming from operational and infrastructure compromise rather than from anything wrong with the cryptography.

Two things are true about this wave, and both belong in this essay. First: *the protocol was untouched.* Every one of these was the periphery — firmware, a swap

service, a payment tool. Bitcoin's consensus rules did what they always do. This is the first essay's Section 4 running live: the network's security is sensor-based, not forecast-based; its weakest points double as tripwires; failures become alarms the whole ecosystem learns from, at a real and terrible cost to the people caught in them. The machines are already probing the human-built edges of the ledger, and the core is holding.

Second, and this is the part the community should sit with: *the moment it was attacked from outside, it pulled together.* The infighting paused. Developers, auditors, rival factions turned outward against a common threat — AnchorWatch pointing AI compute at the infrastructure, the red teams auditing wallets, the whole ecosystem sharing forensics. Give this community an external adversary and its cohesion returns instantly, because cohesion is what an external adversary is *for*. The AI-attack wave is a small, early, involuntary rehearsal of exactly the realignment this essay argues for. The enemy that unifies is not fiat. It is the arrival of machine-speed adversaries — and, one step up, machine-speed minds whose values no one can read.

8. The one who never lost focus

There is one figure in this story who has been, by turns, the community's hero and its villain, and who has in fact been doing the same thing the entire time. I want to use him as a mirror, not a saint — I am not litigating whether his ends are good; that is not the point and I do not know the answer. The point is that he kept his focus while the community turned its own inward.

Michael Saylor understood early that he faced two extrinsic risks he could not control: prohibition and confiscation. He cannot vote them away; they are decisions that belong to others. So he did the only two things available to a man who cannot control the die but can load it. He accumulated — past eight hundred thousand coins — until confiscating him would mean confiscating a systemically entangled mass of institutional capital, until he was, in the old phrase, too big to fail quietly. And he made the accumulation transparent and evangelical — publishing the playbook, urging other treasuries to do the same — so that if the day of confiscation ever comes, he will not be alone on the scaffold; he will be one of many, and moving against him will mean moving against a coalition. He functioned politically: education, advocacy, presence. He could not remove either risk. He made both politically expensive.

He packaged it brilliantly — "digital credit" is not a slogan but a genuine insight, because money has always, in the end, been credit. And watch what the community that once cheered him — because they thought he was pumping the dollar price to the moon — now says about him. When Strategy sold coin to meet obligations, the same crowd that crowned him began to call him a traitor. They had misread him from the start. They thought he was playing *price.* He was playing *survival.* The cheer and the jeer are the same error, read forwards and backwards.

Notice, finally, where Saylor stood when BIP-110 came. He opposed it — "110 Reasons BIP-110 Is a Bad Idea" — on the ground of neutrality: that the network must not start deciding which transactions are worthy, that fee markets and relay policy, not consensus changes, are where such questions belong. So did Adam Back, who had called the proposal a dangerous precedent for changing the protocol by bypassing consensus. And when the fork came and died in two blocks, the post-mortems noticed something new about Bitcoin's governance: the economic majority now includes corporate holders whose preference for protocol stability proved decisive. His opposition was not commentary. It was weight — weight he had spent five years accumulating, doing exactly what it was accumulated to do. The man the community was busy branding a traitor was, on the one question that actually touched Bitcoin's neutrality, defending the exact property this essay says is Bitcoin's entire future value. He did not lose the thread. The loud part of the community did.

9. What to do with the gift

So here is the Monday morning of it — what a Bitcoiner does differently the day after reading this, whether you build, hold, or teach.

First, stop pretending your coins are the thing at risk. They are not — the protocol will be fine with or without you. *You* are the thing at risk. Sit honestly with the arrival of AGI and then ASI, and follow it to the end of the line: if we do not build a workable coexistence between humans and machine intelligence, Bitcoin becomes exactly as irrelevant as we do. Bitcoin will not mind. The protocol is what it is; a machine intelligence may even use it, because a permissionless ledger of unforgeable commitments is close to the only language such a mind natively trusts. But *your human interest* in Bitcoin — your hope that it changes your life, your children's inheritance, your freedom — that interest is only worth something in a world where humans still matter. Coexistence is not Bitcoin's problem to solve. It is yours. Bitcoin does not need you to survive. You need the coexistence to survive.

Second, do the work you are uniquely placed to do. You already understand the hardest part — why a neutral, unownable, fixed registry matters, why verification beats trust, why keys are sovereignty. That is precisely the knowledge the AI-safety world is missing and the Bitcoin world is sitting on without knowing its second use. Combine it. Learn enough about the alignment problem to see where your existing knowledge already answers it. You are closer to the frontier of this than you think; you have simply been pointing your expertise at the wrong enemy.

Third — and this is the hardest and the most important — turn the narrative outward, and tell it first to the people who used to be your opponents. The big-blocker you fought, the institutional buyer you sneered at, the regulator you cursed, the state you wanted to starve: in the coexistence frame they are not your enemies. They are your allies, because they will need the neutral anchor exactly as much as you do, and sooner than you think. The community's reflex is to guard the gift jealously, to police who is a "real" Bitcoiner, to fight over the estate. The

stewardship the gift actually asks for is the opposite: to widen the circle deliberately, to hand the second nature to precisely the actors the first narrative taught you to hate — because it is only by aligning their interests with the anchor's survival that you reach the real goal behind Bitcoin at all. You do not protect the gift by building walls around it. You protect it by making it indispensable to everyone, including the people you were sure were the enemy.

Fourth, and most concretely: go where the plan is being written, and offer the layer you already have. The people drafting the verification architecture publish their work openly and ask for contributors; the AI verification field is small, underfunded and explicitly looking for help. You do not need to become an alignment researcher. You need to show up with the one thing your world has that theirs does not: sixteen years of a running, unowned, non-backdatable record that no state has been able to edit. Anchor your own commitments and show that it works — a lab's evaluation report, an exchange's proof of reserves, a treasury's holdings attestation, a deprecation promise. Build the plumbing between attested hardware and the chain so that anchoring a declaration is one command rather than a research project. Fund it. And when you argue for it, argue in their language: not revolution, not the end of central banking, but *verification between parties who cannot trust each other* — which is, if you strip the slogans away, the only thing Bitcoin has ever actually done.

The community received something almost no group in history has received: a coordination tool of genuine, lasting neutrality, founded through renunciation, that no one had to trust because anyone could verify. It was given the way the best gifts are given — by someone who then disappeared, so that no one could mistake the gift for its giver. To spend that inheritance fighting over blockspace, while the loudest voices brand its defenders traitors, is to hold the gift without the respect its size demands.

There is a second nature to what you hold. It was invisible in 2009 because the mind it anchors *between* had not yet arrived. It is arriving now. The task is to see it before the window opens — to change the story from a war with the past into an anchor for the future, and to carry that story to your former enemies as the allies they have quietly become.

The counterweight already exists. You are holding it. The only question left is whether you understand what it is for before someone with less love for it, and a clearer view of its second nature, understands first.

The strongest refutation of this argument is worth more to its authors than any agreement. If it is wrong, say why.

Appendix: verification, versioning, contact

Verification. This document deliberately contains neither its own hash nor the transaction that anchors it — a document that included its own fingerprint would, by including it, change the fingerprint. The SHA-256 hash of this canonical file, the anchoring transaction (OP_RETURN prefix ANCHOR-V2), its block height, and an OpenTimestamps proof are published in the verification manifest at this document's canonical home. To verify: obtain the canonical file, compute sha256sum, and compare against the OP_RETURN payload of the listed transaction. The anchor is funded from the change of the first essay's dialogue anchor: every artifact of this authorship forms a single, unbroken chain of transactions, checkable end to end.

The first essay. *The Last Scarce Good — constitutional scarcity as a coordination point between humans and machines.* Canonical home: https://nullius2140.github.io/the-last-scarce-good/ — anchored in block 960856.

Authorship. Written by Nullius 2140 in dialogue with Claude (Anthropic). A hash-commitment of the human author's legal identity is anchored separately (block 960869), permitting later proof of authorship without present disclosure.

Versioning. This document is V1.0, the first published and anchored version. Substantive revisions will be published and anchored as V1.1, V1.2, … — the chain serves as the version history. Errata that change the hash change the version.

Contact. Through the canonical home of this document and the channels listed there. nullius2140@proton.me