AfterFiat
The Load-Bearing Thesis

What would be worth holding
when the promises bend

Jason St George

Privacy, Proofs, and Compute may support an agency-preserving bearer asset. Whether they do—and whether they should share one asset—is an empirical question. The thesis does not ask to be believed; it asks to be measured.

Brief 4.1 · reads thesis version 4.0

31 October 2026

Status of This Edition

This is the brief: the AfterFiat thesis told for a first reading. It condenses the canonical full version 4.0 thesis into prose and leaves out its thresholds, formulas, and measurement contracts. The Argument Edition gives the case in one sitting; the full edition is the record. The previous brief, version 4.0, remains available as a technical condensation. **If wording, scope, definitions, thresholds, or interpretation differ, the canonical full version 4.0 thesis governs.**

© 2026 Jason St George. Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). "AfterFiat," "VerifyPrice," "VerifyReach," "VerifySettle," "VerifyFlow," and related marks remain trademarks/service marks of the author and are not licensed under CC BY 4.0.

Citation: Jason St George. *AfterFiat: The Load-Bearing Thesis*. Brief 4.1, 31 October 2026, reading thesis version 4.0. DOI 10.5281/zenodo.18902696.

Contents

The Promise Behind the Promise 1

Three Things Worth Keeping 1

Who Wants It to Fail 2

Why Anyone Would Hold It 3

Insurance that works in the middle . . . 4

Money nobody needs to inspect . . . 4

The unit people reckon in . . . 5

Useful Is Not Money 5

What Gets Through 6

How It Dies 6

What to Build, and What to Buy 8

The Promise Behind the Promise

Every monetary epoch begins with an argument about what is real.

Ours is an argument about promises. Almost everything that lets a modern life move rests on somebody's word. The custodian will honour the withdrawal. The platform will carry the post. The court will enforce the indemnity. The vendor will keep the phone booting. The state will leave the door to exit open. Call these soft guarantees: promises kept by reputation, regulation, and habit rather than by physics or mathematics.

Soft guarantees rarely break. They bend. Nothing is banned. A default changes, a compliance rule tightens, a paragraph in the terms of service is revised, and a rail that was optional becomes the only one that works. The thesis calls this administrative repression, and its mark is that the infrastructure keeps running. The courts sit. Payments clear. The lights stay on. The guarantees are honoured, selectively, on terms someone else sets.

Several pressures are merging into one. A state with debts it cannot honour in real terms will prefer repression to default. Money increasingly comes with compliance attached. Platforms flooded with synthetic media prefer managed truth to open verification. The most capable machines sit behind a few doors, and the power and chips to run more of them are scarce. Each pressure frays the guarantees, and each holds them on a shorter leash.

So the question is old and newly urgent. When the promises bend, is there anything worth holding that keeps working? The thesis does not answer with a forecast. It answers with a claim, put up to be tested:

> **The claim under test.** Under sustained administrative and financial repression, a bearer asset may earn monetary premium if holding it preserves private settlement, portable proof, and access to verified compute after ordinary substitutes weaken. The full service path must remain stress-deliverable; demand must not bypass the asset; a persistent, self-custodied, loss-bearing holder constituency must absorb residual financial risk; and project credit must remain separate. Whether any network satisfies those conditions—or whether the triad should share one asset—is an empirical question. This thesis does not ask to be believed. It asks to be measured, and it names in advance every reading that would retire it.

Two terms carry the claim. A bearer asset is one you hold yourself rather than a balance someone keeps for you; a monetary premium is value beyond anything the asset's cash flows explain.

Now read the verbs. *May* earn. *If* holding preserves. *Must* remain, *must* not bypass, *must* absorb. Every word that carries weight is a condition, and the first condition is the plainest. The infrastructure could succeed without any new money at all. The question is whether *holding* a particular asset gives you something the infrastructure alone does not. Above all: does a balance held in advance do better than holding Bitcoin and buying what you need on the day? The thesis does not assume the answer. It designs an experiment to find it.

Three Things Worth Keeping

Strip away the vocabulary and the thesis is about three capacities a digital life cannot do without.

The first is **privacy**: paying someone without the payment being read over your shoulder, by a competitor, a platform, or a state that has decided to take an interest. Not secrecy from everyone, always. Disclosure you choose, scoped to whoever needs to see it.

The second is **proof**: a fact that carries its own evidence. A computation ran as claimed; a record is what it says it is; a rule was followed. Anyone can check it, cheaply, without asking the party that made the claim.

The third is **verified compute**: machine work that arrives with its receipt, so that capacity becomes something you can count, price, and hold a provider to.

The thesis calls the three together the triad. None of them is money. They are services, and the thesis takes care never to promote a service into a currency by renaming it. Whatever ties them to money has to run through one quantity: what it costs to check.

Gold earned its monetary career on a dark stone. Streak a nugget across it and the mark tells you, in seconds, roughly what you hold; weigh it and the density tells you the rest. Gold was expensive to produce and cheap to assay, so it was expensive to fake against a buyer who ran both checks. That gap, costly to make and cheap to check, is the whole technical basis for public truth at scale, and the thesis's premium rests on it staying wide. When checking a claim costs as much as making it, you no longer have verification. You have a priesthood, and you are back to taking someone's word. The thesis measures the gap directly, as a published price for checking a standard piece of work, and calls it VERIFYPRICE.

Around those three services the thesis builds a small, strict cast, and much of its discipline is keeping each member in role:

- The **base asset** is a bearer asset that might, under conditions, earn a monetary premium. It is a candidate, never a promise.
- **Work Credits** are prepaid tickets for service: capacity reserved with a named provider and used up when the work is delivered. Nobody should treat them as savings.
- **Receipts** are evidence that something happened. They can be copied. They are not scarce, and they are not money.
- **Project notes** are loans for building things. They carry maturity and default, and they must say so.

One concession comes first, before any critic can make it. Bitcoin is the better money. The triad offers different goods, and nobody yet knows whether those goods will carry a monetary premium. Nobody outside Bitcoin buys its work, so nobody can bargain the cost of it down. Useful work brings a customer, and a customer is a lever. The thesis does not argue that Bitcoin is superseded. It asks whether a second asset, tied to goods Bitcoin does not try to supply, can earn a premium of its own. It accepts that the answer may be no while the technology succeeds anyway.

Who Wants It to Fail

The adversary in this story is not a villain. It is a state under financial strain doing what such states have historically done: reaching for the levers within reach. Negative real rates. Capital controls. Custody rules, identity mandates, hardware standards, app stores, cloud contracts, the queue for a grid connection. The likely instrument is not prohibition. It is the default setting, the benefits rule,

the institutional mandate, the platform term: the optional rail made mandatory in practice while it stays optional on paper.

A subtler adversary arrives as a rescuer. When a data centre, a grid project, or a chip line fails, someone with a balance sheet steps in. It may be a strategic patron, a national champion, the state itself. The infrastructure survives, under new owners and new terms about which proofs count and who may connect. The thesis calls this enclosure by rescue. It may be more dangerous than open attack, because the rescuer can be well funded, technically excellent, and genuinely useful.

The strongest competitor is not a failing state but a competent one: a closed system that knits energy, industry, compute, identity, and payments into one machine and runs it well. It may win on cost, on speed, on uptime. The thesis does not claim to beat it on capability. It claims something narrower. Settling without an intermediary, disclosing only what you choose, carrying your proofs elsewhere, and leaving are distinct properties, and a closed system withholds them because withholding them is what makes it closed. Two systems can post the same throughput and the same uptime and give opposite answers to one question: can you leave with your keys, your assets, and your proofs? That question belongs on the scoreboard.

There is a newer buyer on the field, and it is not a person. Software agents now hand tasks to other agents at machine speed. They cannot telephone a reference or wait for a court. The only assurance that fits inside the hand-off is a receipt the delegating machine can check for a fraction of what the work cost. That is why the thesis expects more and more of verification's buyers to be machines, and why it counts that demand only where the hand-off goes to a party the sender could not hold to account except through the protocol.

The machine buyer brings the thesis's strangest failure with it. An agent can hold a wallet, build a reputation out of receipts, and post collateral: every measurable trait of a good holder. Meanwhile the person behind it quietly stops mattering. The key root is not held by a person, and revocation is a request rather than an operation. Or every key stays with a person who never uses it, because a bad outcome after overriding the machine is charged to the person, and a bad outcome after following it is charged to the machine. Both routes read green on every dashboard. The thesis calls the result standing inversion and reads standing as a pair: whether a person can still revoke the agent, and whether the holdings move as one policy. Humans holding every root while their machines move as one is standing exercised by nobody.

The world these adversaries work in comes in four weathers, each with its own readings. Market repair can succeed: private substitutes remain credible, and the premium for an open stack (the three services run on networks anyone may use and anyone can verify) may narrow. Physical bottlenecks in energy, transformers, and shipping can block the repair. Repair can fail, and repression follow. Or a competent closed stack can stabilize everything, at the price of custody and exit. These are observables, not dates.

Why Anyone Would Hold It

Most arguments for a new money stop at usefulness. This one starts where a valuation model runs out. Fees, burns, and collateral can be valued as cash flows, and whatever a cash-flow model can price is not a monetary premium. So the claim rests on three mechanisms such a model does not

reach. Each comes with an instrument to measure it and a red line that can retire it.

Insurance that works in the middle

In ordinary times, a solvent custodian you can sue is an excellent substitute for a cryptographic proof. Courts work. Custodians redeem. Cloud providers are cheap and contractually answerable. For most commercial needs the open stack's advantage is thin.

The advantage changes when the substitute cannot be sued, will not stay solvent, is itself the adversary, or causes a loss no damages can repair: censorship, seizure, deplatforming, disclosure. Then the plain ability to transact, prove, hold, and exit becomes valuable, precisely because the institution that used to provide it has weakened. A holder gets that ability by holding. It is not paid out; it is kept, the way a store of grain is worth more than its price in a lean month.

Pressure alone does not create it. Under little pressure the old substitutes work and the ability is worth little. Under extreme pressure the power, the networks, the hardware, and the exits can fail along with everything else. If the premium lives anywhere, it lives in the band between, where the substitutes weaken and the open stack still runs. The thesis draws this as an inverted U, not a slope: more crisis does not mean more premium. The shape carries an uncomfortable corollary. This is insurance whose underwriter is exposed to the insured event, which is why the physical delivery of the service belongs to the monetary argument and not to an engineering appendix.

How large is it? Nobody knows, and the thesis says so. What it publishes instead is the instrument that would size it: what borrowers pay for temporary access to the asset, read against a published index of regime pressure. It also publishes a red line that can retire the claim, but only once a study with the power to see the effect has looked and found too little.

One alternative deserves its own answer, because it is the one a sceptic reaches for first. Why hold the asset at all, rather than hold Bitcoin and buy what you need on the day? Against that, holding buys exactly one thing: a balance that stays spendable when buying one on the day is unavailable, too slow, or would break the privacy and control the transaction needs. It buys no capacity, no price, and no priority; those are sold separately, as Work Credits. The thesis tests the difference with an access experiment. It runs first on a network that already exists and charges fees in its own coin, with equal budgets fixed before a disruption: a held balance against Bitcoin bought on the day, and against Bitcoin converted by the provider. If Bitcoin does as well, the mechanism is absent for that workload and that kind of stress. The thesis treats that as its default expectation, not as an anomaly.

Money nobody needs to inspect

The second mechanism is older than any coin. An asset behaves like money when nobody gains anything by inspecting the particular unit in front of them. Every money-like asset so far got there by symmetric ignorance: checking a particular unit cost more than it was worth, so nobody looked, and it held only until someone did. Cheap public verification offers the opposite route. Checking costs nothing and anyone can do it, so inspecting gives no one an edge.

The prediction is narrow, and Bitcoin shows why. Its units are perfectly checkable, yet lenders still take haircuts of 30 to 50 per cent against it, because haircuts price volatility and no verifier can compress volatility. So the thesis does not predict lower haircuts. It predicts less *disagreement* among

lenders who underwrite independently, and faster agreement after a shock, than on a comparable whose backing nobody can see. If cheap checking cannot do even that, a red line records it.

The unit people reckon in

The third mechanism is the stickiest thing money does, and the one Bitcoin has not achieved: being the unit people write prices in when nobody makes them. Bitcoin's own miners, seventeen years in, still quote their revenue in dollars and pay their bills in dollars. The thesis holds itself to a harder test than the asset it most admires. If outsiders decline to reckon in the unit, the claim is weakened. If, at the stage when they ought to, the protocol's own insiders will not price their short-term obligations in it, the claim is dead.

Useful Is Not Money

A protocol can route value into its asset in familiar ways. It can require the asset for fees, burn part of what is paid, make providers post it as collateral, and fix its issuance in advance. These matter: they decide where economic value goes. They do not decide whether the asset is money. A burn is a buyback by another name. Collateral is a lockup that lasts while operators stay solvent and choose to stay, and it places no bid. Together they make a valuable service asset, a share of a fee stream plus capital held on a balance sheet, which an ordinary cash-flow model can price without help. None of that turns a payment network, a pipeline, or a clearing house into money, and none of it does so here.

The fee has a ceiling of its own. Proving costs real resources, so the open path starts at a cost disadvantage. A customer routes through it only when what it is worth to them (checkability, neutrality, rules nobody can change at whim, the ability to leave) exceeds that extra cost plus the fee. Bypass is a magnitude, not a switch. The customers who value it most come in two kinds that do not add up: supervised firms that need evidence, and parties beyond a court's reach that need absence. Each one's requirement disqualifies the other, because they share the crowd they hide in. Against a fork of the same open code, the only thing left to charge for is coordination.

A humbling fact in the record is already a decade old. In exactly the repression states this thesis is about, savings fled into dollar stablecoins, not Bitcoin and not a privacy coin like Zcash, settling at scale with no native monetary asset in the loop. For the median need, the incumbent channel is cheaper, faster, and already deployed. The open stack's case survives only in the upper band: private settlement where a stablecoin is a custodial IOU, proof where it is silent, and compute where it has nothing to verify.

Price is no proof either. The protocol and its price are different machines. One supplies the services and routes their demand into the asset. The other wraps the asset in funds, custody claims, futures, and leverage, and sells exposure to people who will never touch the network. Either can move without the other. A rising chart can be a wrapper's success and a protocol's failure at once, and the end of that road is an asset that has become a reference price with no native loop. Price is something to explain, not evidence to cite.

What Gets Through

Crude oil is not diesel when the refinery is the bottleneck. Savings are not long-term funding when no balance sheet will carry the risk. A hall of accelerators is not a service when the power, the cooling, the firmware, the network, or the settlement fails. The thesis makes this a rule.

> **Gross capacity is not deliverable service.**

What counts is the flow that still gets through the narrowest link nobody can route around, after a particular storm has hit. The thesis calls it Delivered Verified Capacity and is strict about it. A substitute counts only if it arrives before the promise expires. Facilities that look independent count as one if they share a transformer vendor, a firmware signer, a cable, or a market maker, or if they answer to the same controller, creditor, or jurisdiction. Nameplate power and installed hardware are not evidence. And the service promised to customers may never exceed a cautious share of what survives the worst published scenario.

The whole argument is laid out as eleven premises and a chain of nine links. The chain runs from demand that persists, through standard workloads, cheap receipts, service that survives stress, open markets, and recurring fees, to an asset that captures those fees, a constituency that holds it through losses, and, only at the end, a premium. Each link names how it fails. The weakest are marked rather than hidden: whether useful work standardizes, whether open markets form around the receipts, whether service survives stress at scale, how much demand bypasses the asset, whether a real holder base forms, and the premium itself.

Who holds the asset matters more than how much of it is bought. A dollar of fee demand is not a dollar of risk absorbed. Users can buy the asset a moment before paying a fee and hold nothing after. Providers can sell what they earn the moment they earn it. A wrapper can create price exposure without anyone holding a key. The anchor the thesis looks for is a constituency that keeps the asset in its own custody, can bear a loss without a margin call, stays well beyond any single transaction, and adds when pressure rises rather than after the recovery. Spending the asset on the service in a storm is the mechanism working, not a holder leaving. And a cohort that is one operating policy spread across many addresses, or that no person can still revoke, is no anchor, however patient it looks.

Somebody also has to pay for the reactor. Long-lived infrastructure needs real credit: underwriting, covenants, maturities, and a holder willing to bear time. The base asset must never become that bond, and Work Credits must never become disguised construction loans. A protocol that let them would walk back into the trap it was built to escape. Money stays free of maturities and coupons. Credit stays labelled and bears its own losses.

> **Proofs** audit the credit. They do not become the bond.

How It Dies

A thesis that cannot be killed is a press release. This one publishes eighteen red lines: named conditions, most of them read on a published series with a threshold and a clock, all of them published

before any reading. One bad quarter ends nothing. The rule is a sustained breach and a failed recovery. Not every line kills, either. Red Lines 7 and 9 and Condition A of Red Line 18 weaken the claim, and every other line kills it. Several lines read only once the network reaches the stage at which they mean something; before then they are published and trip nothing.

Read by what they watch, the eighteen sort into a few families.

The touchstone goes dark.

Checking a standard claim stops being cheap, or the evidence about physical facilities turns opaque.

The exits fail people.

A refund route leaves an honest party without a safe way out; handing over private histories becomes a condition of ordinary life; or lawful privacy proves unusable where it matters.

One hand on the switch.

Verification or compute concentrates in one vendor, a few clouds, or one jurisdiction, or the power to run it is curtailed against it.

The scoreboard is captured.

The data stops being public and checkable, or governance can rewrite issuance, fees, or the measurements without hard limits.

The value never arrives.

Fees never come to pay for security while demand stays speculative; use grows while the asset is bypassed; the premium for checked service, less the cost of checking it, falls below what the protocol charges; wrappers become the asset; or a price fall turns into a collateral spiral.

The money never appears.

The three mechanisms read null on their own instruments: no insurance value in the band, no less disagreement among lenders, no one reckoning in the unit.

Every line, with its threshold and time window, is stated in full in the Complete Edition; the Argument Edition summarizes the first fifteen in a table and prints the three monetary lines whole.

A failed remediation on a line that kills moves the asset from store-of-value candidate to speculative or experimental. On a line that weakens, the claim is restated without the leg that line removes. There is a quieter verdict too: the stack works, capacity is used, fees arrive, and still holding it buys no insurance in a storm. Then the honest name for the asset is a verified-capacity service asset, not money.

The failure most worth fearing would arrive with every dashboard green. It is two threats at once: services from a competent closed stack, and price from the wrappers. The base asset becomes a reference price with no native loop. The thesis watches for it years before any single red line trips, as three things diverging together: exposure outgrowing use, no added value in holding as pressure rises, and the share of capacity run by open, independent operators falling while the closed stack's service improves.

The thesis is as plain about what it has not shown. It has not shown that the three services should share one asset, that a fee can survive bypass, or that burns create savers. It has not shown that the open stack stays physically available in the states where it matters most, or that its insurance value is large, or larger than what gold and Bitcoin already earn. It has not shown that a held balance beats Bitcoin converted on the day for any workload, or that the median buyer will pay for cryptographic

proof while courts and creditworthy indemnitors still work.

And it carries an empty precedent column. No equity-like claim on a fee stream is known to have crossed into monetary premium. Warehouse receipts and bills of lading acquired price and liquidity and never acquired moneyness. Commodities did cross. Silver, salt, grain, and tobacco became money along the path Menger described, on which a good comes to be accepted for its saleability rather than its use. That path is an argument for the possibility. It is not a precedent, and the thesis does not pretend it is.

What to Build, and What to Buy

If the claim is to be tested, something has to be built to test it, and the order matters. First come the receipts and a test harness anyone can rerun, so the scoreboard exists before anyone is scored. Then one private settlement corridor, made refund-safe, before any second one. Then one proof factory with a standard starter set of workloads, then the tools developers build with; the access experiment runs beside them, on a network that already exists. Neutral routing follows, and with it the evidence about physical facilities. Useful-work pilots come last, and they exist to study an open problem rather than to announce a money. Adoption advances on telemetry, not on a calendar. The build itself is promised by the quarter. Until the stack passes its first published maturity test, the base asset is research exposure, and a working stack is simply infrastructure. Only the later tests make the asset a candidate at all.

That fixes what is on offer. The verifiable stack, and the institution that measures it, are fundable as public infrastructure now. The measurement layer has prospective buyers who need not hold a token, and part of it could be sold against existing Bitcoin wrappers before any base asset exists. The base asset is something else: an option to learn, not an underwriting, with eighteen published ways to die. The record names the lab proposed to build and measure the stack, Kardashev Labs, and publishes the lab's own kill conditions beside the thesis's. It offers no token, no treasury, and no early exposure.

The thesis ends on a mandate rather than a forecast. Build receipts, rails, and verifiable machines. Measure the whole path, from energy to the holder. Keep self-custody and exit. Keep credit separate. Find out who actually bears the risk. And retire or downgrade the claim when its published conditions fail.

Privacy equips people to transact without being legible by default. Proofs equip them to check claims without trusting a platform. Compute equips them to buy machine work without a single gatekeeper. Telemetry equips the public to see when any of these promises becomes another soft guarantee. Where people act through agents, equipping them means a key they hold and a revocation they can actually use.

Gold condenses geology. Bitcoin condenses thermodynamics. The triad may condense verifiable agency in the band where institutions weaken but networks still work. The first two are established monetary facts. The third remains an experiment.

Where to read next

The Argument Edition
The case in one sitting: the mechanisms, the chain, the objections, and the red lines.

The Complete Edition
Every threshold, formula, measurement contract, and source. Where any edition differs, it governs.

The trip wires
Each red line with what it reads, at afterfiat.xyz/tripwires/.

The essay
Who Holds the Keys When the Guarantees Fail: the instrument panel for the transition, at afterfiat.xyz/essay/.