The Adversarial Default

Josh · Secure Sovereign

Published August 20, 2026

A Defense of Toxic Maximalism

Contents

The criticism is familiar by now. Bitcoin culture is toxic. The maximalists are hostile, uncharitable, and harsh toward anyone who asks questions they've already decided are stupid. Newcomers get bitten. Researchers get dismissed. Developers who wander in from other crypto scenes leave with scars. The advice that follows is always some version of the same thing: be more welcoming, be more charitable, assume more good faith. Grow up.

This article is a defense of that hard default. Not every insult and not every pile-on — some of that is noise — but the stance itself. **The hostility is correct.** It matches the threat. People asking Bitcoin to soften have not faced what the hostility is defending against.

I. What Being Collaborative Actually Produced

The case for a friendlier Bitcoin culture is not really philosophy. It is a claim about what friendliness delivered the last time people tried it. So look at the record.

The blocksize war did not start because maximalists woke up one morning and decided to be difficult. It followed years of trying to work inside a process that could be captured — and was. Developers who raised concerns about one dominant codebase, who pays the developers, and who gets to approve code changes were not rewarded for honesty. They were pushed to the margins. Their proposed changes were closed. Their concerns were reframed as attacks on the project. The people who stayed civil and trusted the process watched that process deliver exactly what the hostile critics had predicted.

Taproot is the other side of that coin: an upgrade that was largely uncontested. The features were popular — better privacy and smarter scripts — and the fight was mostly about how to turn it on, not whether the rules themselves were a good idea. Soft culture treated that as a win. Hard review of what the new surfaces could become was thin.

SegWit's cheaper witness data and Taproot's removal of the old script-size ceiling made large data payloads practical. The Taproot "envelope" — an `OP_FALSE OP_IF` branch that never runs — was meant as an upgrade hook, not a file store. Ordinals and inscriptions used it anyway. JPEGs and token junk went into the chain. Non-money data is now an estimated 12 to 19 percent of total chain storage. Spam blockspace ran roughly 17 times its pre-inscription baseline. About 29.6 percent of UTXOs are inscription-related while holding only around 415 bitcoin. Every validating node pays for that forever. A soft fork almost nobody fought still put lasting abuse on the chain. For the cost model and what consensus can still close, see *Bitcoin Is Not a Hard Drive* and *The Achievable Floor*.

The OP_RETURN fight in 2025 ran the same script as the blocksize war, after that abuse was already real. Ready proposals to close dedicated ways of stuffing non-money data into blocks — rules every validating node must accept — stalled. Core v30 removed the limit on how much `OP_RETURN` data nodes would forward. The stronger technical case did not win. A small set of funded people with power over Bitcoin Core treated doing nothing on those protections as the default, and treated social pressure as a stand-in for technical debate. The constructive side lost to how the system is built, not to a better argument.

This is not ancient history. It is what both collaboration and soft celebration of "uncontested" upgrades produced when tested for real. The hard stance critics call toxic came after that evidence, not before it. It followed the failures. For the blocksize-war outcome and the OP_RETURN timeline, see *Governance Paralysis Was The Victory* and *Who Controls Bitcoin, §V*.

II. What a Softened Culture Costs on the Outside

Who controls Bitcoin Core is not the only argument. There is a second defense critics almost never meet head-on, because it means admitting the hostility protects people who are not even in the room.

Bitcoin maximalists call things scams. They do it loudly, early, and with little patience for the charge that they are being unfair to founders. In most cases they are right. The people who disagreed with them at the time went on to lose money — sometimes a lot, sometimes everything.

MIT Sloan estimates the Terra ecosystem collapsed in three days in May 2022 and wiped out about $50 billion in value. Reporting at the time put the Terra/Luna wipe near $45 billion overnight. FTX took customer deposits trusted to an exchange whose founder Fortune had put on its cover as a

possible "next Warren Buffett," then went bankrupt in November 2022. The SEC later charged that customer funds had been diverted to Alameda without disclosure. Celsius, Voyager, and BlockFi followed the same pattern at smaller scales. The Chicago Fed documents withdrawal freezes and bankruptcies across those platforms, with hundreds of thousands of customers owed in each filing.

In every one of these cases, maximalists had been calling it early, loudly, and in the same tone critics call toxic. In every one of these cases, the culture that wanted Bitcoin more welcoming to other crypto projects gave promoters cover.

The hard default is a warning system. When it is loud and consistent, it is harder to run a project that borrows Bitcoin's credibility. When it softens, the warning gets weaker, and ordinary investors pay. Destroyed savings and retirement funds are not abstract. After Terra, reporting documented people describing total loss and mental-health crisis, including thoughts of suicide on public forums (Time; Al Jazeera). Those costs fall on people who never asked for a friendlier culture. The same pattern shows up when famous names replace checking the work: reputation becomes cover. See *Don't Trust, Verify* and *The Last Uncaptured Asset*.

III. Why Bitcoin Needs This Tone

Inside Bitcoin, the hard stance fits what Bitcoin actually is.

Bitcoin is hard to undo at scale. A bad code merge. A quiet bug. A captured group of Core gatekeepers shipping a change that helps their funders. A soft fork almost everyone liked that opens an abuse path. Once any of that ships and spreads, there is no network-wide undo button. Being wrong in Bitcoin costs more than being wrong in most other engineering work. That gap is not small. Harsh public pressure on proposed changes, hard looks at who people are and what they want, and open challenge of anything that touches the money rules are rational responses — including upgrades that look uncontested. The other option is a nicer culture that is also a more dangerous one.

This is not theory. Bitcoin Core 30.0 and 30.1 had a wallet migration bug that, under specific conditions, could delete all files in the wallet directory when an unnamed legacy `wallet.dat` migration failed, with no recovery if backups did not exist. Bitcoin Core's own advisory states the risk of fund loss and pulled the affected downloads. The dangerous `fs::remove_all` pattern had been introduced years earlier. In 2024, Core maintainer ryanofsky named the exact risk in code review, said what it could do, and recommended a follow-up fix. No follow-up was created. A later change removed an earlier accidental stop that had been blocking the dangerous path. Users lost wallets. The fix landed in PR #34156 after the bug was reported (issue #34128).

This was not a clever crypto attack. It was a known-dangerous pattern a maintainer had named and flagged, left sitting for a year, until it ran. The process a softer culture would ask Bitcoin to trust more fully let a named warning sit until people lost funds.

CVE-2018-17144 makes the same point for the money rules themselves. An inflation bug that could have created Bitcoin out of thin air sat in the live software for roughly eighteen months before disclosure. Bitcoin Core's September 20, 2018 notice documents it. A second Bitcoin node program, written separately and checking the same blocks, would have caught it right away. Other clients existed on paper. None were widely used for that job. Almost everyone ran Core. That is what left the bug alive. The same one-client setup that left the inflation bug hidden for eighteen months left the wallet warning unfixed for a year. The threat has not gone away. The tone matched to it should not soften either. Full accounts of both failures are in *Don't Trust, Verify* and *Who Controls Bitcoin*.

IV. The Inflation Problem

Not all Bitcoin conflict does useful work. Call this the other inflation problem: fights that grow with no way to settle them in code. A lot of what looks like ideology is really two people arguing about what the protocol actually says, without a clear written standard. That is a question you can answer if you have the right tool.

No such tool exists. Bitcoin Core has never produced a clear mathematical write-up of the rules every node must enforce. Fifteen years of capable, well-funded developers on software that secures trillions of dollars, and still no formal specification. So every fight about what Bitcoin is, and what it allows, stays in arguments and reputation instead of settling in code. Heat with no finish line and no appeal. The fight cannot end because there is no written standard that can end it.

That noise weakens the warning the hard default is supposed to give. When everything is a battle, the person who spots a real threat gets drowned out next to the person performing tribalism. Questions that have technical answers bleed into the alarm system and make it harder to hear.

A formal write-up of the consensus rules moves that slice of conflict out of social combat and into engineering, where evidence can settle it. The necessary conflict stays. Fights about values, what can go wrong, and priorities are real and should stay hard. The conflict that is really just unclear protocol text shrinks when you give it a standard. That is an engineering fix that also lowers the noise. It is not a call to be nicer. See *Why Bitcoin Needs a Specification* and *The Social Layer Is the Attack Surface, §VI*.

V. The Fight Is Not Over

People asking Bitcoin to soften are implying the threat that produced the hard default has passed — that governance is mature enough now, that the hostility is a leftover from an earlier, riskier period Bitcoin has outgrown.

None of that is true.

The one-software problem is intact. Roughly 99% of nodes that matter still run software from the Core line: Bitcoin Core itself, plus programs forked from Core such as Knots. Knots showed that operators will switch over what transactions a node forwards. It is still a Core fork, not a separately written program that decides the money rules on its own. No separately written Bitcoin software, proven to follow the same money rules, has enough of the network running it to matter.

Who pays for Core development is still concentrated. A small number of grant organizations, with documented ties to companies and funds that care about protocol outcomes, still pay most Bitcoin Core development. Who merges code is still concentrated too. Brink's Engineering Impact Report 2025 shows one person at one organization merged 56% of all changes to Bitcoin Core in 2025; Bitcoin Governance Research shows the same shape in the 2022+ window (~50% top-1, ~83% top-3). The right to merge into Bitcoin Core is still a small fixed set — currently five people on bitcoin/bitcoin; live GitHub permissions are the source of truth. A subpoena, a regulatory order, or a quiet talk with that set can still move a protocol change the rest of the network can do little about.

None of the conditions that made the hard culture appropriate have gone away. The trauma that produced it was real. The threat is ongoing. The engineering that would give the conflict a healthier shape is still being built. There is still no formal specification the economy actually runs on. There is still no separately written second Bitcoin client, proven against the same money rules, with enough of the network running it to matter. Forks of Core that only change what they forward do not close that gap. The funding map and the path off the monopoly are in *Who Controls Bitcoin* and *Governance Paralysis Was The Victory*.

The hard default is Bitcoin's immune system. It matches a threat that has not gone away. It is not a personality disorder. Critics calling it toxic are asking the patient to drop the fever before the infection clears. The fever is doing work. Leave it alone until the structure changes. Then we can talk.

Companion to The Social Layer Is the Attack Surface, Who Controls Bitcoin, Governance Paralysis Was The Victory, Don't Trust, Verify, Why Bitcoin Needs a Specification, The Achievable Floor, Bitcoin Is Not a Hard Drive, and Bitcoin Governance: Argument Map.

Sources

- Liu, Makarov, and Schoar, "Anatomy of a Run: The Terra Luna Crash," MIT Sloan CFI — Terra ecosystem collapse in three days, ~$50B valuation wiped
- Al Jazeera, "After Terra, Luna crashes, regulators count cost of crypto", May 20, 2022 — ~$45B Terra/Luna erase; retail savings wiped
- Time, "What Terra's Crash Means For Crypto and Beyond", May 2022 — retail losses; public forum reports of suicidal ideation after the crash
- Fortune, "30-year-old billionaire Sam Bankman-Fried… next Warren Buffett", August 1, 2022 — pre-collapse magazine celebration
- SEC press release 2022-219, December 13, 2022 — charges that FTX customer funds were diverted to Alameda
- Chicago Fed Letter No. 479, "A Retrospective on the Crypto Runs of 2022" — Celsius, Voyager, BlockFi, FTX withdrawal pauses, bankruptcies, customer counts
- Bitcoin Core, "Wallet Migration Failure May Delete Unrelated Wallet Files", January 5, 2026 — official advisory for Core 30.0 / 30.1
- bitcoin/bitcoin#34128 — wallet migration deletion bug report
- bitcoin/bitcoin#34156 — fix removing `fs::remove_all` cleanup
- Bitcoin Core notice, CVE-2018-17144, September 20, 2018 — inflation bug disclosure
- Brink Engineering Impact Report 2025, March 26, 2026 — 56% merge concentration
- Bitcoin Governance Research — merge concentration, stalled proposals, conflict-resolution findings

SECURESOVEREIGN

Markdown is the canonical source: https://secsov.com/articles/the-adversarial-default/index.md

Formatted snapshot of https://secsov.com/articles/the-adversarial-default

Josh · Secure Sovereign