Why Shitcoins Are Shitcoins

Josh · Secure Sovereign

Published August 17, 2026

A research report on the structural failures of altcoins as monetary assets

Contents

I. Introduction

Thousands of alternative cryptocurrencies have been launched since Bitcoin. Almost none have survived as meaningful stores of value. Seventeen years and multiple market cycles have produced the same outcome often enough that the failure pattern looks structural, not like a collection of one-off post-mortems.

Altcoins fail as monetary assets. Launching a new chain does not replicate Bitcoin's properties, whatever the founder's sincerity or the elegance of the design. That is not the same as calling every token worthless for every purpose. Some power smart contract platforms and stablecoin rails with real usage and volume. Whether that justifies an independent consensus layer is taken up at the end. The argument throughout is the monetary asset case.

The question is not whether an altcoin has interesting technology. It is whether its rules have held up under real adversarial pressure, not just been described as decentralizable on paper. What follows applies that test across security, enforceable rules, decentralization under fire, monetary credibility, founder dependence, securities exposure, market survivorship, and workloads that may not need their own chain at all.

II. Security

Bitcoin's security rests on its accumulated hashrate, representing billions of dollars of capital investment in specialized SHA-256d hardware deployed over seventeen years. MIT Digital Currency Initiative monitoring and industry estimates put the capital cost of acquiring enough SHA-256 hashrate to attack Bitcoin in the tens of billions of dollars, with only a tiny fraction of that hashrate ever available on rental markets. No credible 51% attack has ever been mounted against the Bitcoin base chain.

A new proof-of-work chain starting from scratch has none of that. Its hashrate on day one is a fraction of Bitcoin's, which means the cost to attack it is a fraction of what it would cost to attack Bitcoin.

Altcoins with thin hashrate get attacked. In January 2019, Coinbase documented fifteen deep reorganizations on Ethereum Classic, twelve of which included double spends totaling 219,500 ETC (~$1.1 million at the time). ETC was hit again in August 2020, when separate attacks double-spent roughly 807,000 ETC (~$5.6 million) and 238,000 ETC (~$1.7 million) using hashrate rented from NiceHash. Bitcoin Gold, whose stated purpose was restoring mining decentralization, suffered ~$18 million in double-spend losses across May 2018. Verge suffered two mining attacks in April and May 2018 that exploited timestamp bugs to mint millions of XVG at artificially low difficulty. The second attack alone was estimated at roughly $1.7 million. As of August 2026, XVG trades more than 99% below its December 2017 all-time high and has never meaningfully recovered. For many smaller tokens, the hashrate needed for a 51% attack is available for rent on NiceHash at a cost below the profit from a successful double-spend. The MIT DCI has documented that pattern across dozens of PoW altcoins.

A chain can accumulate hashrate over time, but most never do. The point is not that every new chain gets attacked, but that it remains attackable in a way Bitcoin is not, and that gap degrades the security model whether or not an exploit ever lands.

Proof-of-stake chains with large accumulated staked value present a different but still weaker case. Ethereum, after years of real usage and billions in staked ETH, is not equivalent to a fresh launch. Staked capital and mined hashrate are different kinds of security. Hashrate represents sunk physical investment that cannot be instantly liquidated or redirected. Staked capital can be withdrawn, slashed, or concentrated by well-capitalized actors in ways that specialized mining

hardware cannot. Ethereum's social contract has already proved negotiable. The July 2016 DAO hard fork reversed settled transactions because the community decided the outcome was unacceptable. That is a different security model than Bitcoin's, not an equivalent one. The monetary case against Ethereum as a store of value is developed below.

III. Rules Without Enforcement Are Gibberish

A blockchain's entire value proposition rests on one claim, that its rules are enforced without a trusted administrator. Remove that claim and you have an inefficient distributed database with no compensating advantage.

For that claim to mean anything, the rules must be practically impossible to change without overwhelming consensus. Bitcoin's rules have that property. Its accumulated hashrate makes a hostile takeover economically irrational, and its diverse global node network means no single actor can dictate protocol changes. The rules have been tested by well-funded adversaries and held.

A chain susceptible to 51% attack does not have that property. If whoever rents enough hashrate on a given afternoon can rewrite transaction history, the rules are not rules. They are suggestions that happen to be currently uncontested. A system where any sufficiently motivated actor can change the ledger at will is not trustless. It has anonymous, unaccountable administrators who operate without legal liability and without any mechanism for recourse.

This is worse than an openly centralized system. A permissioned database with known administrators gives users recourse. The administrators are identified, legally accountable, and replaceable. A thin-hashrate blockchain delivers the appearance of trustlessness while providing a system where the rules bend to whoever can assemble a temporary majority. It combines the inefficiency of distribution with the unreliability of unaccountable administration.

IV. Decentralization: Potential vs. Reality

A system can be designed to be decentralizable without actually being decentralized, and the gap between those two things is where almost every altcoin spends its entire existence.

Bitcoin's decentralization is not something you read off a diagram. It was produced under sustained adversarial pressure from governments, exchanges, competing developer factions, and hostile miners across seventeen years. It survived the blocksize war, the SegWit activation fight, multiple nation-state mining bans, and repeated attempts by well-funded actors to redirect its development. Each of those fights hardened the social consensus around Bitcoin's rules. Bitcoin's

reference-client governance is concentrated. That is a separate problem from the one addressed here. What altcoins lack is seventeen years of demonstrated monetary rule persistence at the network level.

A new chain has survived none of that. Its founding community is typically ideologically homogeneous, assembled around a shared narrative or grievance, which means it has never faced the internal disagreement that actually reveals whether a social contract is durable.

Decentralization metrics often count nodes or validators and miss who actually controls the network. On Ethereum, liquid staking protocols, exchange-operated staking, and foundation treasuries cluster influence in ways headline dashboards hide. Lido's share of staked ETH fell from roughly 32% in 2023 to near 24% by 2026 after sustained community pressure. That confirms the concentration concern rather than resolving it. The relevant test is whether a social contract survives when that concentration becomes visible, not whether marketing copy says "decentralized." Named foundations holding large token treasuries add another administrative layer. Those entities can vote on rules that directly affect the supply they control. A chain that has never faced those tests at comparable scale has not demonstrated decentralization. It has demonstrated a founding coalition that agrees with itself.

V. Monetary Policy Credibility

Bitcoin's 21 million supply cap is credible not because it exists in the code but because the social consensus defending it has been tested repeatedly and held. Every attempt to change Bitcoin's monetary policy has failed. That was not because of technical barriers. The human network defending those rules is large, diverse, and economically incentivized to maintain them. Bitcoin has adopted consensus upgrades, including SegWit and Taproot, without reversing settled transaction history or altering the supply cap. The 2017 Bitcoin Cash fork was the direct test of whether monetary rules could be overridden by a well-funded minority. The network rejected it. Ethereum's 2016 DAO hard fork, by contrast, reversed settled ledger history when stakeholders decided the outcome was unacceptable. That distinction matters for the monetary asset case. Slashing and validator penalties on proof-of-stake chains police behavior within accepted rules. They do not prevent the rules themselves from being rewritten under social pressure.

Most altcoins carry a softer version of this commitment. Their monetary policy is defended by smaller, younger, more homogeneous communities that have not faced equivalent pressure. Many launch with low circulating supply and large unlock schedules. Early buyers hold paper gains while insiders and treasuries distribute into liquidity. Continuous issuance on most L1s, and repeated inflation-schedule changes on chains like Solana, mean holders depend on ongoing demand to absorb new supply. Ethereum's issuance model has changed several times, including the post-

merge shift to burn-linked issuance. That remains a governance decision, not a fixed rule etched under fire. A supply cap defended by a community that has never been seriously tested is a stated intention, not a demonstrated commitment. Stated intentions are not sound money.

VI. The Founder Problem

Almost every altcoin was founded by an identifiable person or small group whose preferences shaped the protocol and whose identity became inseparable from the community's. Ethereum has Vitalik Buterin. Solana has Anatoly Yakovenko. That follows naturally from starting a project with a specific technical or ideological agenda rather than releasing a neutral monetary protocol into the wild.

Bitcoin is structurally different. Its founder disappeared early, leaving no living authority to appeal to, defer to, or override. No one can claim to speak for Satoshi, and that absence removes a pressure point every living-founder chain keeps exposed. Bitcoin's rules are defended by the network itself rather than by the ongoing preferences of any individual.

Chains with living founders inherit the founder's judgment, relationships, and ongoing role in governance, formal or not. Regulators, institutions, and the community treat the founder as the project's public decision-maker. That creates a pressure point on a single identifiable person. Bitcoin's absent founder structurally resists that. When founders exit, pivot, or disagree with the community's direction, the resulting instability has played out dozens of times in altcoin history.

VII. Securities Risk

Almost every altcoin token was issued through an ICO, presale, foundation allocation, or founder reserve. In each case, investors bought an asset expecting profit from someone else's work. That is the Howey test, and most altcoins fail it in ways Bitcoin does not. The SEC has pursued dozens of enforcement actions against unregistered token offerings; federal courts have applied Howey transaction-by-transaction rather than treating crypto assets as a single category (*SEC v. Coinbase*, 2024).

Bitcoin was never sold in a presale. There was no ICO, no foundation allocation, no founder's reserve. Coins entered circulation only through mining, available to anyone willing to contribute hashrate from day one. In March 2025, the SEC staff explicitly distinguished proof-of-work mining from investment-contract offerings, noting that miners earn rewards from computational work rather than passive reliance on a promoter’s managerial efforts.

Regulatory liability does not have to materialize for this to matter. The existence of securities exposure creates uncertainty for exchanges, institutional holders, and downstream applications that Bitcoin does not carry. That uncertainty is priced in even when regulators have not yet acted.

VIII. The Price Record

CoinGecko's dead-coins study found that 53.2% of all cryptocurrencies listed on GeckoTerminal between July 2021 and December 2025 are no longer actively traded. In 2025 alone, 11.6 million tokens went inactive after recording at least one trade. That accounted for 86.3% of all failures in that five-year window. Minted-but-never-traded projects were excluded. The fourth quarter of 2025 saw 7.7 million failures, concentrated after the October 10 liquidation cascade that wiped out roughly $19 billion in leveraged positions in twenty-four hours. The figure includes many tiny, abandoned, or spam projects, but the direction is clear. The overwhelming majority of crypto projects fail.

Across the more established end of the market, cycle-to-cycle survivorship screens put the share of altcoins that fail to reclaim a prior cycle high above 80%. MEXC analysis of prior cycle tops found roughly 20% of cryptocurrencies hit a new all-time high from one cycle to the next, implying 80% did not. TradingKey cites similar token-survivorship data across major cycles. As of mid-2026, CryptoQuant analyst Darkfost's "altcoins near ATL" screen tracks tokens trading below 25% of their all-time high. It put the figure near 40%, briefly climbing toward 45% when Bitcoin fell below $60,000 in June 2026. These are snapshot figures. Treat them as directionally consistent rather than precise. They hold across multiple data sources and multiple cycles.

No altcoin has matched Bitcoin's multi-cycle appreciation against the dollar. A handful of large-cap names, including Ethereum, BNB, and Solana, have reclaimed prior cycle highs in dollar terms. Even those tokens have lagged Bitcoin when measured peak to peak across the same windows. The clearest example is Ethereum. ETH/BTC peaked near 0.148 in June 2017, reached roughly 0.087 in November 2021, and traded near 0.027 by mid-2026. Each cycle high in Bitcoin terms was lower than the last, even when ETH reclaimed dollar highs. Outside that small set, dollar recovery from one cycle high to the next is rare. That is what you would expect from assets that lack Bitcoin's security, monetary credibility, network effects, and institutional depth.

IX. Bitcoin Dominance as the Macro Signal

Bitcoin dominance, the share of total crypto market capitalization held by Bitcoin, has ranged from 94% in April 2013 down to ~33% at the peak of ICO mania in January 2018. It has since recovered to the 56-58% range in 2026. Every altcoin narrative cycle plays out the same way. ICOs, DeFi summer, NFTs, L1 fee wars, AI agents. Dominance falls during the frenzy as capital rotates into speculative assets. Then it recovers as the narrative exhausts itself and the money retreats to Bitcoin.

That reversion is not a temporary anomaly. Capital leaves Bitcoin chasing narrative returns in alts, then comes back when the narratives run out of road.

The institutional infrastructure now being built around crypto concentrates around Bitcoin. U.S. spot Bitcoin ETFs absorbed a record $18.7 billion in net inflows in Q1 2026 alone. Cumulative net inflows since the January 2024 launch exceeded $65 billion by mid-2026. Ethereum spot ETFs launched in July 2024, but cumulative institutional flows have remained far below Bitcoin's. The wrapper does not erase ICO-era distribution or the monetary-policy problems described above. CoinShares 13F analysis found registered investment advisors accounting for 57% of institutional Bitcoin ETF holdings. Average reported portfolio allocations were still below 1% of AUM, leaving substantial room for further inflows that have historically favored Bitcoin over altcoin baskets. Sovereign treasuries hold Bitcoin, not altcoin baskets. The U.S. Strategic Bitcoin Reserve holds roughly 328,000 BTC from forfeitures. El Salvador (~7,700 BTC) and Bhutan (~3,100 BTC) are among the few nation-states with verifiable on-chain holdings. None of that infrastructure transfers to alternative chains by virtue of their existence.

X. The Lindy Effect and Network Effects

Bitcoin's value proposition compounds with time in a way that cannot be replicated by launching a new chain. Every year Bitcoin survives, the credible commitment that it will continue to survive strengthens. Nassim Taleb called that the Lindy effect, the observation that the longer something has survived, the longer it is likely to continue to survive.

Institutional capital already flows toward Bitcoin first, as the previous section showed. The point here is that the advantage compounds and does not transfer. A new chain has no Lindy effect and no deep derivatives markets, global exchange depth, or custody rails. Those took years of adversarial survival to build. They were assembled incrementally by actors with strong economic incentives to build on the chain that already had liquidity. They are not rebuilt from scratch on a new ticker.

XI. On Smart Contracts and the Blockchain Problem

The standard defense of non-Bitcoin blockchains is that they serve different purposes. Smart contracts, decentralized applications, programmable money, tokenized assets, stablecoin infrastructure. Some of that is real. Stablecoins on Ethereum, Solana, and Base move real transaction volume. Certain DeFi primitives have persistent usage. USDC settles on all of those chains. The asset is the issuer's dollar liability. The chain is just transport. You do not need to own ETH or SOL as monetary assets to use it, any more than SWIFT messages require you to own the bank software they ride on.

What makes a blockchain worth the cost is narrower. Censorship resistance, permissionlessness, immutability without a trusted administrator, and a monetary policy no one can override. Those properties are expensive in efficiency, throughput, and complexity. They are worth paying for

when participants genuinely cannot agree on a trusted third party and when the cost of administrative interference is high enough to justify the inefficiency. Speed and low fees are database properties. They do not by themselves justify a separate consensus layer with its own token.

For most use cases built on smart contract platforms, a permissioned distributed database with known administrators is faster, cheaper, more efficient, and provides legal accountability that a blockchain cannot. Administrators can fix bugs, reverse errors, and be held responsible, which is exactly what you want when accountability matters.

The DAO hack makes the trade-off concrete. When a smart contract vulnerability drained roughly 3.6 million ETH (~$60 million at the time) from The DAO in June 2016, Ethereum executed a hard fork at block 1,920,000 to reverse the theft and move the stolen funds into a recovery contract. That was the right practical decision and a clear demonstration that the system has administrators who operate through social consensus rather than legal authority. Ethereum is not trustless in the way Bitcoin is trustless. As a store of value it asks you to trust that its social consensus will continue to protect your holdings. Bitcoin asks you to trust math and accumulated hashrate.

Trustless computation among mutually distrusting parties is a real problem. Atomic composability, global transaction ordering, and censorship-resistant inclusion are all easier inside a single consensus domain today than across separate systems. Engineering convenience and architectural necessity are not the same thing. A single consensus domain may make certain workloads easier to implement today. That does not automatically justify a permanent separate chain with its own token, founder risk, weaker security model, and demonstrated willingness to bend its rules under social pressure. A temporary implementation advantage does not clear that bar. Zero-knowledge proofs, multi-party computation, validity proofs, and Bitcoin-anchored execution schemes continue to separate the computation problem from the consensus problem. Projects launching independent consensus layers today are betting their current convenience outlasts those alternatives. They accept every structural disadvantage already described.

When you trace the non-monetary requirements that actually hold up, the list is short. Timestamping, proof of publication, existence proofs, settlement finality, credible neutrality in adversarial coordination settings. They all point toward anchoring to Bitcoin's demonstrated security rather than replicating it at a fraction of the cost on a weaker chain. For the design-purpose case against treating chains as general-purpose platforms, see *Bitcoin Is Not a Hard Drive*. For which non-monetary workloads consensus can close on Bitcoin rather than on a separate L1, see *The Achievable Floor*. Timestamping already works this way. OpenTimestamps anchors document hashes to Bitcoin without a separate token or consensus layer. In practice the non-monetary design space resolves to cryptographic protocols anchored to Bitcoin, not to a proliferation of independent chains. What remains is either a permissioned database that should admit what it is, or a temporary engineering convenience that does not justify its long-term costs.

XII. Conclusion

The properties that make Bitcoin Bitcoin are not features in a codebase. They are what seventeen years of adversarial pressure produced when the network passed the tests laid out above. That meant security without goodwill, rules that held under attack, monetary policy that survived forks and politics, fair issuance without promoter dependence, market survivorship that compounded across narrative cycles, and non-monetary use cases that resolve to anchoring rather than launching another token.

No alternative chain replicates that by launch. Security can be written into a white paper. Lindy, institutional depth, and demonstrated social-contract durability cannot. The handful of large-cap survivors that reclaimed dollar highs still lost ground against Bitcoin across cycles. The long tail failed in numbers that no marketing budget can explain away. Most blockchain applications do not need a new monetary layer. They need honest accounting about who administers the system, or cryptographic anchoring to the one chain that passed the monetary tests. Money is the one use case that cannot delegate that choice. Bitcoin is the one chain that has not made it.

Related: The Last Uncaptured Asset, Bitcoin Is Not a Hard Drive, The Achievable Floor, Who Controls Bitcoin.

Sources

Research compiled August 2026.

Security and 51% attacks

- MIT Digital Currency Initiative — 51% Attacks project
- Coinbase — Ethereum Classic double-spend incidents (January 2019)
- CoinDesk — ETC second 51% attack, August 2020
- Bitquery — ETC July 2020 attack analysis
- ZDNet — Bitcoin Gold double-spend attacks, May 2018
- CoinDesk — Verge blockchain attacks, 2018
- CoinGecko — Verge (XVG) price and ATH data

Token failure and altcoin performance

- CoinGecko — Dead coins: How many cryptocurrencies have failed?
- CoinDesk — More than half of all crypto tokens have failed (January 2026)
- MEXC — The Cycle Highs And Cycle Lows (Redfist)
- TradingKey — Why 80% of Altcoins Never Reclaim Their Highs
- CoinMarketCap Academy — CryptoQuant altcoins near ATL screen (Darkfost)

- CF Benchmarks — The ETH/BTC ratio through time

Bitcoin dominance and institutional flows

- Lambda Finance — Bitcoin Dominance History (2013–2026)
- CoinMarketCap — Bitcoin Dominance chart
- Binance Academy — A Brief History of Bitcoin Dominance
- BlockLR — Bitcoin ETF Performance Q1 2026
- CoinShares — 13F Bitcoin ETF institutional report, Q3 2025
- Bitcoin Reserve Tracker — sovereign holdings
- WealthManagement.com — RIA crypto ETF exposure

Securities regulation

- SEC — Statement on Certain Proof-of-Work Mining Activities (March 2025)
- SEC — Unicoin offering fraud charges (2025)

Ethereum governance

- CoinDesk — The DAO attacked (June 2016)
- Ethereum Foundation — Hard Fork Completed (July 2016)
- CoinDesk — Lido staking share and validator concentration (August 2025)

Bitcoin-anchored utilities

- OpenTimestamps

SECURESOVEREIGN

Markdown is the canonical source: https://secsov.com/articles/why-shitcoins-are-shitcoins/index.md

Formatted snapshot of https://secsov.com/articles/why-shitcoins-are-shitcoins

Josh · Secure Sovereign