Fiat-Backed vs Crypto-Backed Stablecoins

Two models, one supposedly the decentralised answer to the other — and the awkward fact that the challenger now holds mostly the same assets as the incumbent.

Alain AI Lab Research · Published July 29, 2026 · 10 min read

The choice between a stablecoin backed by dollars in a bank and one backed by crypto locked in a smart contract has always been presented as a choice between trusting a company and trusting code. It is a real distinction, and for years it was the central argument in this sector. What makes the comparison interesting now is that it has partly dissolved: the leading crypto-backed system holds only a minority of its collateral in crypto, with the larger part in tokenised government debt and in another issuer's fiat-backed token. Understanding why that happened tells you more about the two models than any list of features. It assumes you know what a stablecoin is.

AT A GLANCE

FIAT-BACKED **Reserves at a company**	CRYPTO-BACKED **Over-collateralised on-chain**	REAL DIFFERENCE **Who can freeze your tokens**
COST OF THE SECOND **Capital inefficiency**	WHAT HAPPENED **The models converged**	NOW DECIDED BY **Censorship resistance, mostly**

01

The two designs, in brief

A fiat-backed stablecoin is a claim on a company. You give it a dollar, it holds a dollar of cash or short-term government paper, and it issues you a token redeemable for that dollar.

Solvency is a question about the company's balance sheet, and you verify it by reading disclosures.

A crypto-backed stablecoin is a claim on a smart contract. Users lock crypto worth substantially more than the tokens they issue against it, and if the collateral falls toward the danger threshold, it is sold automatically to keep the system whole. There is no company holding your money, no bank account, and no redemption department — solvency is a question about collateral ratios and liquidation mechanics, and you verify it by looking at the chain. Both designs are described more fully in our overview; what follows is the comparison.

02

Where they genuinely differ

Five axes matter. On *counterparty risk*, the fiat-backed model concentrates it in one company and its banks, while the crypto-backed model replaces it with smart contract risk and collateral risk — different exposures, not fewer. On *transparency*, the crypto-backed system wins decisively: anyone can verify the collateral in real time, whereas a fiat-backed issuer's reserves are visible only through periodic attestations, with the limits discussed in what are Tether's reserves.

On *capital efficiency*, the fiat-backed model wins decisively: one dollar in, one token out, versus locking up considerably more value than you issue. On *failure mode*, the two break differently — a fiat-backed token fails through reserve shortfall or a blocked redemption route, a crypto-backed one through collateral collapsing faster than liquidations can clear, particularly during network congestion. And on *censorship*, the difference is categorical rather than a matter of degree, which is why it deserves its own section.

03

The axis that actually decides it

A fiat-backed issuer can freeze tokens at a specific address. This is not a flaw or an accident — it is a designed capability, exercised in response to law enforcement requests, and it is a condition of operating as a regulated financial institution. If you hold a fiat-backed stablecoin, your balance exists at the discretion of a company that can render it unusable, as our note on whether an issuer can freeze your holdings examines.

A properly decentralised crypto-backed system generally cannot do this. There is no administrator with a freeze function, because the tokens are issued by a contract against collateral rather than by an entity maintaining a ledger of who may transact. For most users, most of the time, this difference is invisible and irrelevant. For anyone whose reason for using this technology is that they do not want a company able to switch off their money — people in jurisdictions with capital controls, in politically exposed positions, or simply holding a principled view — it is the entire point, and no amount of capital efficiency compensates for it. This single axis explains why the crypto-backed model persists despite losing on nearly every other measure.

> *The crypto-backed model was built to avoid depending on a company holding dollars in a bank. Its flagship now holds the larger part of its collateral in tokenised government debt and in another company's fiat-backed token — which is a serious answer to a question about efficiency, and a quiet abandonment of the question it was created to answer.*

04

Why the second model never scaled

The crypto-backed approach has remained a small fraction of the stablecoin market, and the reason is structural rather than a failure of execution. Issuing a token requires someone to lock up more value than they receive, which means supply can only grow when people want leverage against their crypto holdings. Demand for the stablecoin itself cannot create supply — only demand for borrowing can.

That is a severe constraint. A fiat-backed issuer can meet any amount of demand by accepting more dollars; a crypto-backed system can only meet demand if enough people want to borrow against volatile collateral, which tends to collapse precisely when demand for stable assets peaks. Add the capital cost of over-collateralisation, the operational demands of managing vault positions, and the complexity facing an ordinary user, and the ceiling becomes clear. It is a well-engineered mechanism serving a naturally limited market.

05

The convergence

Which brings us to the development that reframes this entire comparison. Faced with that ceiling, the leading crypto-backed system began accepting collateral that was neither volatile nor crypto: first the fiat-backed stablecoins of centralised issuers, held directly in a facility allowing direct swaps to defend the peg, and subsequently tokenised real-world assets — principally short-term government debt, the same instruments a fiat-backed issuer holds.

The result is that the flagship decentralised stablecoin now holds only roughly a fifth of its backing in actual crypto assets. The remainder is split between tokenised government paper and a centralised competitor's token. Critics have made the obvious observation that this makes it, to a substantial degree, a wrapper around another issuer's reserves plus treasury exposure — and that characterisation is difficult to dispute on the numbers. The decentralised alternative has, in the most literal sense, converged on the model it was designed to replace.

06

Why it happened

It is worth resisting the temptation to read this as betrayal, because the pressures were real and each decision was defensible on its own terms. Holding a centralised stablecoin as collateral, accessible through a direct swap facility, is by far the most effective tool available for defending a peg — it restores the primary-market anchor that a purely collateral-based design lacks, as described in how stablecoins stay pegged. Tokenised government debt earns a return that funds the protocol and lets it pay holders a savings rate, which is a genuine competitive advantage no fiat-backed issuer may lawfully match in the United States — the prohibition examined in how stablecoin issuers make money.

And both moves relaxed the supply ceiling that volatile-collateral-only design imposed. So the protocol traded decentralisation for stability, revenue and scale — each individually rational, cumulatively transformative. The lesson generalises well beyond stablecoins: decentralisation is expensive, its costs are paid continuously while its benefits appear only in rare adverse events, and systems under competitive pressure will tend to trade it away one reasonable decision at a time.

07

The regulatory asymmetry

Regulation has reinforced the same direction. The United States framework for payment stablecoins is built around issuers holding high-quality liquid reserves and honouring redemptions — requirements that a company can satisfy and that a smart contract, having no legal personality, cannot straightforwardly meet — the statutory scheme set out in what is the GENIUS Act. European analysis has similarly questioned whether the governance of major decentralised protocols satisfies the relevant criteria.

The practical consequence is that the fiat-backed model has a clear path to authorisation and the crypto-backed model largely does not, which determines which tokens regulated exchanges, payment firms and institutions can offer. That is not a judgement about which design is safer — the crypto-backed model's transparency is genuinely superior on one axis regulators claim to care about — but about which one fits a framework written for institutions. Combined with the yield advantage that has drawn the crypto-backed system toward treasury collateral, the regulatory landscape pushes both models toward the same place.

08

What remains, and how to choose

Despite the convergence, a real difference survives, and it is the one from section 03. Even a crypto-backed token holding substantial centralised collateral typically retains no administrator able to freeze an individual holder's balance. Your tokens cannot be switched off, even if the assets behind them are increasingly conventional. That is a narrower claim than the model's original promise, and it is not nothing.

So the choice reduces to a short set of questions. If you want maximum liquidity, the simplest risk assessment, and regulatory acceptance, the fiat-backed model is straightforwardly better and the market has said so decisively. If your priority is that no company can freeze your balance, the crypto-backed model still offers something its competitor structurally cannot — but check what actually backs it now, because the answer has changed and may not be what you assumed. And if your reason for preferring it was that its collateral was not government paper held by intermediaries, that reason has substantially expired. The honest summary is that this was a genuine debate that the market, the mathematics of capital efficiency, and regulation have largely settled — leaving one narrow but real distinction for the people who need it.

“The thing that hath been, it is that which shall be… and there is no new thing under the sun.”

ECCLESIASTES 1:9

Methodology & Sources

This report compares two design categories as at the date of publication; it contains no protocol names, token names, market capitalisations, collateral ratios, or precise percentages — collateral compositions change continuously through governance and should be verified against current on-chain data and protocol disclosures. The characterisation of fiat-backed designs as claims on a company holding cash and short-term government paper, and of crypto-backed designs as over-collateralised claims on smart contracts with automated liquidation, is the conventional description of each. The statement that fiat-backed issuers generally retain the capability to freeze tokens at specified addresses, and that decentralised crypto-backed systems generally do not, reflects documented issuer capabilities and protocol architecture respectively; implementations vary and some crypto-backed systems have introduced administrative controls. The supply constraint described — that crypto-backed issuance depends on demand for borrowing against collateral rather than demand for the stablecoin itself — is structural. The convergence described, in which the leading crypto-backed stablecoin came to hold the larger part of its collateral in tokenised real-world assets and in a centralised issuer's fiat-backed token, with only a minority in volatile crypto assets, reflects publicly reported collateral composition and governance decisions at the time of writing; the criticism that this makes it substantially a wrapper on another issuer's reserves is a characterisation advanced by named commentators and is reported as a contested view. Regulatory observations regarding authorisation pathways and decentralisation criteria reflect frameworks and published analysis as reported; these continue to evolve. Nothing here is a recommendation regarding any token, protocol, or trade.

Alain AI Lab — independent crypto & AI research.
intelligencecrypto.org · Research is educational and analytical, not financial advice.