What Is a Stablecoin?

A crypto token engineered to hold a steady value — the three ways that is attempted, the one that keeps failing, and what "backed by dollars" actually has to mean.

Alain AI Lab Research · Published July 25, 2026 · 10 min read

A stablecoin is a cryptocurrency designed to hold a constant value, almost always one unit of a national currency — usually the US dollar. It moves on blockchain rails like any other token, but it is built to be boring: one unit today, one unit tomorrow. That combination of blockchain mobility and price stability has made stablecoins the most heavily used instrument in crypto, the default way value moves between assets, platforms and countries. But "designed to hold a value" is doing considerable work in that sentence, because the methods used to achieve it differ enormously in robustness — and one family of designs has failed catastrophically and repeatedly.

AT A GLANCE

WHAT IT IS **Token pegged to a stable value**	USUALLY PEGGED TO **The US dollar**	TYPE 1 **Fiat-backed — holds reserves**
TYPE 2 **Crypto-backed, over-collateralised**	TYPE 3 **Algorithmic — historically fragile**	PEG HELD BY **Redemption and arbitrage**

01

Why they exist at all

The problem stablecoins solve is specific. Blockchains are excellent at moving value quickly, globally and without permission, but the assets native to them swing violently in price — which makes them poor for the ordinary business of holding money, quoting prices, or

paying someone. Conventional money is stable but sits inside banking rails that are slow across borders, closed at weekends, and unavailable to a great many people.

A stablecoin attempts to take the settlement properties of the first and the price behaviour of the second: something you can send to anyone in minutes at any hour, which will still be worth the same when it arrives. That is why they became the plumbing of the crypto market — most trading pairs are quoted in them, they are the resting place for capital between positions, and they are the collateral layer of most on-chain finance. It is also why their use has spread beyond trading entirely, into remittances and into savings for people whose local currency is unreliable, an adoption story taken up in our note on stablecoin infrastructure.

02

Fiat-backed: the dominant model

The largest stablecoins work in the most intuitive way. A company issues tokens and holds an equivalent amount of conventional assets in reserve — cash and short-term government debt, principally. Each token is a claim: hand one back to the issuer and receive a dollar, and the reserve exists to make that promise good.

The model's strength is its simplicity, and it is why this design dominates in practice. Its weakness is that it is not really a crypto arrangement at all — it is a promise by a company, and the token is only as reliable as that company's reserves, competence and honesty. Three questions therefore decide whether such a coin is sound: what the reserves actually consist of, since cash and short-dated government paper behave very differently from riskier assets under stress; whether their existence is verified by a credible independent party, and how often; and whether you personally can redeem, since in many cases direct redemption is available only to large institutional counterparties while everyone else must rely on selling in the market. Notice what this means — a fiat-backed stablecoin reintroduces exactly the trusted intermediary that blockchains were designed to remove. That trade is often worth making. It should be made knowingly.

03

Crypto-backed: over-collateralised by design

The second family avoids the company by using crypto assets as collateral instead of bank deposits. Because those assets are themselves volatile, the system cannot back one dollar of stablecoin with one dollar of collateral — a fall in the collateral's price would instantly leave

the token unbacked. The solution is deliberate excess: users lock up meaningfully more value than they issue, so there is a buffer absorbing ordinary price declines.

If collateral falls toward the danger point, the position is liquidated automatically to protect the peg, which is why these systems are described as over-collateralised. The appeal is that everything is visible on-chain and enforced by code rather than by a company's word — you can inspect the collateral yourself. The costs are capital inefficiency, since a great deal of value must be locked to issue relatively little, and a dependence on liquidations working properly during exactly the violent, congested conditions in which they are most likely to strain. It is a genuinely different risk profile from the fiat-backed model: less counterparty risk, more market and mechanism risk.

04

Algorithmic: the design that keeps breaking

The third family attempts stability with little or no collateral at all, using code to expand and contract supply in response to price — typically by trading against a second, volatile token issued by the same system. When the stablecoin trades below its peg, the mechanism offers arbitrageurs a profit for removing supply; above it, for adding supply. On paper it is elegant, and it requires no reserves.

In practice this family has a poor record, and the central reason is worth understanding precisely: the design depends on the companion token retaining value, and that value depends in large part on confidence in the stablecoin. When confidence breaks, both fall together, and the mechanism that is supposed to restore the peg instead accelerates the collapse — supply expands into a falling market, driving the companion token down further, which weakens the peg further. This is a reflexive loop rather than a stabiliser, and it has produced sudden, near-total losses, most notoriously in the failure of a major algorithmic stablecoin and its paired token in 2022, an episode that erased an enormous amount of value in days. Newer designs have tried to add partial collateral or other safeguards. Treat the category with real caution: a stablecoin whose stability rests on the market's continued belief in a related token is not the same kind of instrument as one holding government bills, whatever the marketing says.

> *Every stablecoin answers one question: what, exactly, is behind this token, and who has to keep a promise for it to be worth a dollar tomorrow? If the answer is unclear or the*

> *promise depends on confidence in something else, the word "stable" is describing an intention rather than a property.*

05

How the peg actually holds

It is worth being clear that nobody enforces the price of a stablecoin in the open market. It trades on exchanges like anything else, and its price is set by supply and demand there. What holds it near its peg is arbitrage, made possible by redemption.

If a token backed by real reserves trades slightly below a dollar, anyone able to redeem can buy it cheaply and exchange it with the issuer for a full dollar, pocketing the difference — and that buying pushes the price back up. If it trades above, the reverse arbitrage applies. The peg is therefore not a rule but an *equilibrium*, maintained by people profiting from deviations. Two consequences follow. First, the credibility of the redemption route is what makes the arbitrage work: if participants doubt they will actually be paid, they stop buying the dips and the peg slips. Second, small deviations are entirely normal — a stablecoin ticking slightly off a dollar is the mechanism working, not failing. A *depeg* worth worrying about is a large, sustained deviation, and it is usually a market verdict on whether the backing is real.

06

What they are actually used for

Four uses dominate. The first is trading: stablecoins are the quote currency of the crypto market, the instrument prices are expressed in and the place traders sit between positions without leaving the ecosystem — which is why market depth is so often denominated in them, as our note on market liquidity discusses. The second is payments and transfers, particularly across borders, where sending a token can be faster and cheaper than correspondent banking.

The third is access to dollars. For people in countries with high inflation or capital controls, a dollar-denominated token reachable from a phone is a genuinely significant financial instrument, and this is among the fastest-growing sources of real demand. The fourth is on-chain finance, where stablecoins are the dominant collateral and unit of account for lending and other protocols. Notice that only the first is speculative — most stablecoin usage is not

about making money on the token, but about using it as money, which is what distinguishes this corner of crypto from most of the rest.

07

The risks that remain

Five deserve naming. *Reserve risk* is the possibility that the assets behind a fiat-backed token are not what is claimed, or not liquid enough to meet redemptions in a rush — which is why the composition and verification of reserves matter more than any other disclosure. *Counterparty and censorship risk* follows from the same structure: a centralised issuer can generally freeze or seize tokens at specific addresses, a power used against illicit activity and one that means these tokens are not bearer instruments in the way bitcoin is, as our note on whether Tether can freeze your USDT examines.

Depeg risk is the possibility of a sustained break from the peg, whether from reserve doubts, a liquidation failure, or a reflexive collapse. *Regulatory risk* cuts both ways — frameworks in major jurisdictions have brought reserve and disclosure requirements that make compliant coins safer while constraining others. And there is a quieter one: *yield-bearing* variants that pay a return are not simply better stablecoins, because the yield must come from somewhere, and that somewhere is additional risk taken with the backing. A stablecoin paying you to hold it is doing something with the reserves, and you are exposed to whatever that is.

08

How to judge one

Five questions, in order. What backs it — conventional reserves, over-collateralised crypto, or an algorithm? If reserves, what are they composed of, and who verifies them, how often, and how credibly? Can anyone redeem directly, or only large institutions — because that determines whether the arbitrage holding the peg is robust or fragile? What is its history through market stress, since a coin that held through a crisis has evidence behind it that a new one simply lacks? And who can freeze it, under what authority?

Then keep the sensible perspective. Stablecoins are useful and, in the well-collateralised cases, have proved durable through serious turbulence. They are also not bank deposits: there is generally no deposit insurance, no central bank behind them, and the promise is a private one. Treating them as a settlement instrument and a temporary store of value is

reasonable. Treating them as risk-free is not — and the difference between the two is exactly the set of questions above.

“Which hope we have as an anchor of the soul, both sure and stedfast.”

HEBREWS 6:19

Methodology & Sources

This report explains an instrument category and how to assess it; it contains no coin names, issuer names, market capitalisations, reserve figures, yields, or collateral ratios, all of which vary by issuer and change continuously — consult current issuer disclosures and attestations directly. The taxonomy used — fiat-backed tokens holding conventional reserves, crypto-collateralised tokens secured by deliberately excess on-chain collateral with automated liquidation, and algorithmic designs relying on supply adjustment and a companion token rather than collateral — is the conventional classification. The account of peg maintenance is mechanical: market price is set by supply and demand, and proximity to the peg is sustained by arbitrage that depends on a credible redemption route, which is why redemption access and reserve credibility matter more than any stated policy. The characterisation of algorithmic designs as historically fragile, and the reflexive failure mode described, reflects the documented record of that category, including the collapse of a major algorithmic stablecoin and its paired token in 2022; no specific project is named here and readers should consult primary accounts. The observation that centralised issuers can typically freeze tokens at specified addresses reflects publicly documented issuer capabilities, which differ between issuers. Regulatory frameworks referenced in general terms differ by jurisdiction and continue to evolve. Stablecoins are not bank deposits and are generally not covered by deposit insurance. Nothing here is a recommendation regarding any token, issuer, or trade.

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