Bitkaya

BITKAYA RESEARCH — BASELINE SERIES

Stablecoin Fundamentals

A plain-language primer for readers new to stablecoins

July 2026 · Bitkaya Base Line Series

1. What Is a Stablecoin?

A stablecoin is a digital token built to hold a steady value — almost always $1.00 — instead of floating freely like Bitcoin or Ether. Most stablecoins do this by being backed 1:1 by real-world reserves (cash and short-term government debt) held by the company that issues them. Hold one token, and you hold a claim on one dollar of reserves, redeemable through the issuer.

Crypto assets are useful for moving value quickly and cheaply across borders on a blockchain, but their prices swing sharply. Stablecoins solve that: they let a business or person use blockchain rails — fast settlement, 24/7 availability, programmability — while pricing and holding value in familiar dollar terms. That combination is why stablecoins have grown into the most-used category of crypto asset for payments, trading, and remittances.

A short history

Tether (USDT) launched in 2014 as the first widely adopted stablecoin, originally on Bitcoin's Omni layer before expanding to Ethereum, Tron, and many other chains. Circle's USDC followed in 2018 with a heavier emphasis on regulatory compliance and disclosure from the outset. Both grew steadily as crypto trading volumes grew, since exchanges needed a stable asset to price and settle trades against. Growth accelerated sharply from 2020 onward as DeFi (decentralized finance) created new uses for stablecoins as collateral and a unit of account, and again after 2023 as payments and remittance use cases matured. The market's most important stress test came in May 2022, when TerraUSD (UST) — an algorithmic stablecoin with no real reserves — collapsed to near zero within days, wiping out an estimated $40-45 billion in value. That event reshaped the industry: it discredited under-collateralized designs, pushed users and regulators toward fully-reserved models, and set in motion the regulatory frameworks (the US GENIUS Act, the EU's MiCA) that now govern the sector — covered in the companion Quarterly Report.

IN SHORT

A stablecoin is a digital dollar substitute: crypto-speed and crypto-reach, without crypto's price volatility.

2. Who Uses Stablecoins, and Why

Stablecoins started as a trading tool and have since broadened into several distinct use cases, each with a different profile of who's involved and what matters to them:

- Traders and exchanges — the original use case. Stablecoins let a trader exit a volatile position into something stable without leaving the crypto ecosystem or waiting for a bank transfer. Most crypto trading pairs are priced against USDT or USDC rather than the US dollar directly.
- Cross-border payments and remittances — sending stablecoins avoids the multi-day settlement, correspondent-banking fees, and cutoff times of traditional wire transfers. This is especially valuable for migrant workers sending money home and for businesses paying international suppliers or contractors.

- Individuals and businesses in weak-currency economies — in countries with high inflation or capital controls (parts of Latin America, Africa, and Southeast Asia in particular), holding dollar-pegged stablecoins is a practical way to preserve savings without needing a US bank account.
- DeFi (decentralized finance) — stablecoins are the primary form of collateral and the main unit of account across lending, borrowing, and trading protocols built directly on blockchains.
- Corporate treasury and payments infrastructure — an increasing number of payment companies, card networks, and even banks are integrating stablecoins for merchant settlement and treasury management, drawn by 24/7 settlement and lower cross-border costs (see the Quarterly Report's competitive section for current examples).

3. The Main Types of Stablecoin

Fiat-backed / reserve-backed

The dominant model, used by USDT (Tether) and USDC (Circle) — together roughly 82-90% of the entire stablecoin market. A single company holds reserves and mints or burns tokens as customers deposit or redeem dollars. Trust in the token depends entirely on trust that the issuer actually holds what it claims.

Crypto-collateralized

Tokens like DAI or Sky's USDS are backed by other crypto assets locked in smart contracts, over-collateralized (e.g., $150 of crypto backing $100 of stablecoin) to absorb price swings in the collateral. No single company holds the reserves; rules are enforced by code and a decentralized governance process instead. This removes single-issuer counterparty risk but introduces a different risk: a sharp enough crash in the collateral asset can still break the peg if liquidations don't keep pace.

Algorithmic (mostly discredited)

Some earlier stablecoins tried to hold their peg through code and market incentives alone, without full reserves — typically by pairing the stablecoin with a second, freely-floating token that was supposed to absorb demand shocks. The best-known example, TerraUSD (UST), collapsed in May 2022, erasing roughly $40-45 billion in value within a week, when the incentive mechanism failed under stress and both tokens spiraled toward zero together. It remains the industry's central cautionary tale and is a large part of why regulators — and the market — now favor fully-reserved models.

Yield-bearing

A newer category (Ethena's USDe, USDY, BlackRock's BUIDL) that passes reserve or trading income back to holders, functioning more like a tokenized money-market fund than a payment instrument. Worth noting: under the new US and EU rules (see the companion Quarterly Report), a token that pays yield directly to holders generally cannot qualify as a regulated “payment stablecoin” — so the largest, most widely used stablecoins (USDT, USDC) deliberately

do not pay yield to holders themselves, even though the issuers earn substantial interest on the reserves backing them (see Section 4).

4. How Reserve-Backed Stablecoins Actually Work

When a customer sends the issuer $1, the issuer mints one new token and adds the dollar to its reserves. When a customer redeems a token, the issuer burns it and returns a dollar. In between, the issuer typically holds reserves in cash and short-dated government securities so that a) the value is stable and b) reserves can be liquidated quickly if many holders redeem at once.

What reserves are actually made of

Issuer reserve disclosures typically break down into a few categories: cash and cash-equivalents held at banks; short-term US Treasury bills, generally the largest component for the major issuers; overnight repurchase agreements (repo), a short-term secured lending instrument; and, historically for Tether, smaller allocations to corporate paper, precious metals, or other assets — a mix that has narrowed over time toward safer, more liquid instruments as regulatory pressure increased. The quality and liquidity of this mix determines how quickly and reliably an issuer can meet redemptions during a stress event.

Who can actually redeem, and how

Direct 1:1 redemption for dollars is usually only available to institutional or verified counterparties dealing directly with the issuer (often subject to minimum amounts). Most retail holders never redeem directly — instead they sell their stablecoin on an exchange or through a market maker at whatever the current market price is, which is normally extremely close to $1.00 but is not literally guaranteed to be exactly $1.00 at every moment. This distinction — the issuer's redemption guarantee versus the secondary-market price you'd actually receive — matters most during periods of stress.

Issuer economics: why this is a profitable business

Reserve-backed issuers earn interest on the reserves they hold (largely from short-term Treasuries) while paying $0 in interest to token holders. At current market size, this spread is the core of a very large business: Tether alone reported a $1.04 billion profit in Q1 2026 on this model (see the Quarterly Report). Understanding this incentive helps explain both why issuers are motivated to grow circulating supply, and why regulators have focused reserve-quality and disclosure rules specifically on this category of stablecoin.

Attestation vs. audit — a distinction worth knowing

Most issuers publish periodic “attestations”: a snapshot, prepared by an accounting firm, confirming reserves matched liabilities on a given date. This is materially lighter-touch than a full financial audit — an attestation checks a single point in time and does not test internal controls or verify the full history of transactions the way an audit does. Tether has never had a full audit from a major accounting firm, relying instead on quarterly attestations. Circle

publishes monthly attestations and, since going public via IPO in 2025, carries additional public-company disclosure obligations. This gap in disclosure rigor is one of the clearest ways the two largest issuers differ, and is worth factoring into any counterparty assessment.

5. Why the Blockchain ("Chain") Matters

A stablecoin is not a single thing living in one place. Issuers mint the same token — representing the same underlying dollar claim — natively on several different blockchains at once. USDT on Tron and USDT on Ethereum are both genuine USDT, redeemable through Tether, but they live on separate networks with very different cost, speed, and ecosystem characteristics. Because Bitkaya trades and settles on Tron, Ethereum, and Solana specifically, understanding these differences matters directly for execution quality.

What actually happens when you send a stablecoin

A transfer is a message broadcast to the blockchain's network saying "move X tokens from address A to address B." Independent validators (computers running the network's software) check that the sender actually holds the tokens, agree on the transaction's validity through the chain's consensus mechanism, and add it to the next block. Once enough subsequent blocks confirm it, the transfer is considered final and irreversible. The sender pays a small network fee for this processing — called "gas" on Ethereum-style chains — priced in the chain's own native token (ETH, TRX, or SOL), not in the stablecoin itself. This is why the cost and speed of moving USDT or USDC depends entirely on which chain it's moving on, not on the stablecoin itself.

Native issuance vs. bridged tokens

Ideally, an issuer mints a stablecoin natively on a chain — meaning Tether or Circle directly controls the contract and reserves back it 1:1 on that chain. Some tokens instead reach a chain via a third-party "bridge," which locks the original token on one chain and issues a wrapped IOU on another. Bridged tokens carry extra smart-contract and operator risk on top of the underlying stablecoin's own risk, since you're now also trusting the bridge. Bitkaya's focus chains — Tron, Ethereum, and Solana — all have native USDT and/or native USDC issuance, which is one reason they're preferred over chains that rely on bridged versions.

Tron

A high-throughput, low-fee chain using a delegated proof-of-stake consensus model with a small set of elected "super representatives" validating blocks, which is part of why it achieves such fast, cheap settlement. It has become the dominant home for USDT specifically — particularly for retail and remittance use in emerging markets across Latin America, Africa, and Southeast Asia. Blocks finalize in roughly 3 seconds.

Ethereum

The original smart-contract blockchain, running on proof-of-stake consensus with a large, globally distributed set of validators — the source of its reputation as the most decentralized and battle-tested major chain. It remains the

deepest, most institutionally trusted venue for stablecoins overall. Fees are higher than Tron or Solana and finality slower, but liquidity, DeFi integration, and compliance/custody tooling are the most mature of any chain. Most other EVM-compatible chains (chains that can run Ethereum-style smart contracts) trace their tooling and standards back to Ethereum.

Solana

A high-speed, very low-cost chain using a proof-of-stake design with an added timing mechanism ("proof of history") that lets validators order transactions extremely quickly. It has become the fastest-growing base for USDC in particular, increasingly used by banks and payment firms for near-real-time settlement. Fees are a small fraction of a cent and transactions finalize in seconds.

6. Key Risks to Understand

- **Peg / depeg risk** — a token's market price can briefly trade away from $1.00 during stress (USDC did this briefly in March 2023 during a US regional banking crisis, when a portion of its reserves were temporarily stuck at a failed bank).
- **Issuer / counterparty risk** — your ability to redeem depends on the issuer actually holding adequate, liquid, good-quality reserves and remaining solvent and licensed. Retail holders typically rely on secondary-market prices rather than direct redemption (see Section 4).
- **Smart contract and bridge risk** — moving tokens between chains via a third-party bridge, or interacting with DeFi protocols, carries code-level hack and bug risk beyond the stablecoin's own reserve risk.
- **Chain risk** — congestion, outages, or consensus problems on the underlying blockchain can delay settlement, independent of the stablecoin itself.
- **Regulatory / freezing risk** — issuers can and do freeze tokens at specific addresses (for sanctions or crime enforcement), meaning stablecoin balances are not censorship-resistant in the way people sometimes assume; rules are also changing quickly (see the Quarterly Report's regulatory section).
- **Concentration risk** — USDT and USDC together represent the large majority of the market; a serious problem at either issuer would have systemic, market-wide effects given how deeply embedded both are in exchange and DeFi infrastructure.
- **Liquidity / market-depth risk** — even a fully-solvent, well-reserved stablecoin can trade briefly below $1.00 on a specific exchange or chain if sellers temporarily outnumber buyers there and arbitrage hasn't caught up yet.

7. Glossary

Term	Meaning
Peg	The target value a stablecoin is designed to track — typically $1.00 USD.
Circulating supply	The total value of tokens currently issued and held by users (not burned or held in reserve by the issuer).
Attestation	A point-in-time check by an accounting firm confirming reserves match liabilities — lighter than a full audit.
Audit	A comprehensive, formal examination of financial statements and controls — more rigorous than an attestation.
Mint / burn	Creating new tokens on deposit (mint) or destroying tokens on redemption (burn).
Redemption	Exchanging a stablecoin back for the underlying fiat currency directly through the issuer, typically limited to institutional counterparties.
Reserve	The assets (cash, short-term government debt, repo) an issuer holds to back tokens in circulation.
Depeg	A period where a stablecoin's market price diverges materially from its $1.00 target.
Gas fee	The transaction fee paid to a blockchain's network to process a transfer, priced in the chain's native token.
Finality	The point at which a transaction is considered permanent and irreversible on-chain.
Consensus mechanism	The process by which a blockchain's validators agree on which transactions are valid (e.g., proof-of-stake, delegated proof-of-stake).
CCTP	Circle's Cross-Chain Transfer Protocol — burns USDC on one chain and mints it natively on another, avoiding wrapped/bridged tokens.
Energy (Tron)	Tron's resource unit for computation; used instead of directly burning TRX for many transaction types.
Bridging	Moving a token's value from one blockchain to another, typically via a wrapped representation or a burn-and-mint protocol like CCTP.
Wrapped token	A representation of an asset on a chain it wasn't natively issued on, backed by the original asset locked elsewhere — carries extra bridge/operator risk.
EVM-compatible	A chain that can run Ethereum-style smart contracts, letting it reuse much of Ethereum's tooling and standards.
DeFi	Decentralized finance — lending, borrowing, and trading protocols built directly on a blockchain rather than through a traditional financial intermediary.
Proof of reserves	Public evidence (an attestation, on-chain data, or an audit) that an issuer's reserves match its circulating token supply.
Whitelisting	A list of addresses an issuer has approved for a specific privilege, such as direct redemption — most retail addresses are not whitelisted.

Disclaimer

This document was prepared by Bitkaya for general informational purposes only and is provided to its intended recipient(s) on that basis. It reflects publicly available information and Bitkaya's understanding of the stablecoin market as of July 28, 2026. The stablecoin market, and the regulatory environment around it, change quickly; Bitkaya does not undertake to update this document for developments occurring after that date.

Nothing in this document constitutes investment, financial, legal, tax, or other professional advice, and it should not be relied upon as the basis for any decision. It is not, and should not be construed as, an offer, solicitation, or recommendation to buy, sell, hold, or otherwise transact in any asset, token, or security. Readers should seek independent professional advice suited to their own circumstances before making any financial, legal, or tax decision.

Bitkaya has used reasonable efforts to ensure the information in this document is accurate and drawn from sources it believes to be reliable, but makes no representation or warranty, express or implied, as to its accuracy, completeness, or currency. Certain figures are explicitly marked as estimates, or as derived from other published data, because they could not be independently verified from a single authoritative source at the time of writing; these should be re-verified before any external, regulatory, or decision-making use. Past performance and historical market data are not indicative of future results. To the fullest extent permitted by law, Bitkaya accepts no liability for any loss arising from any use of, or reliance on, this document.