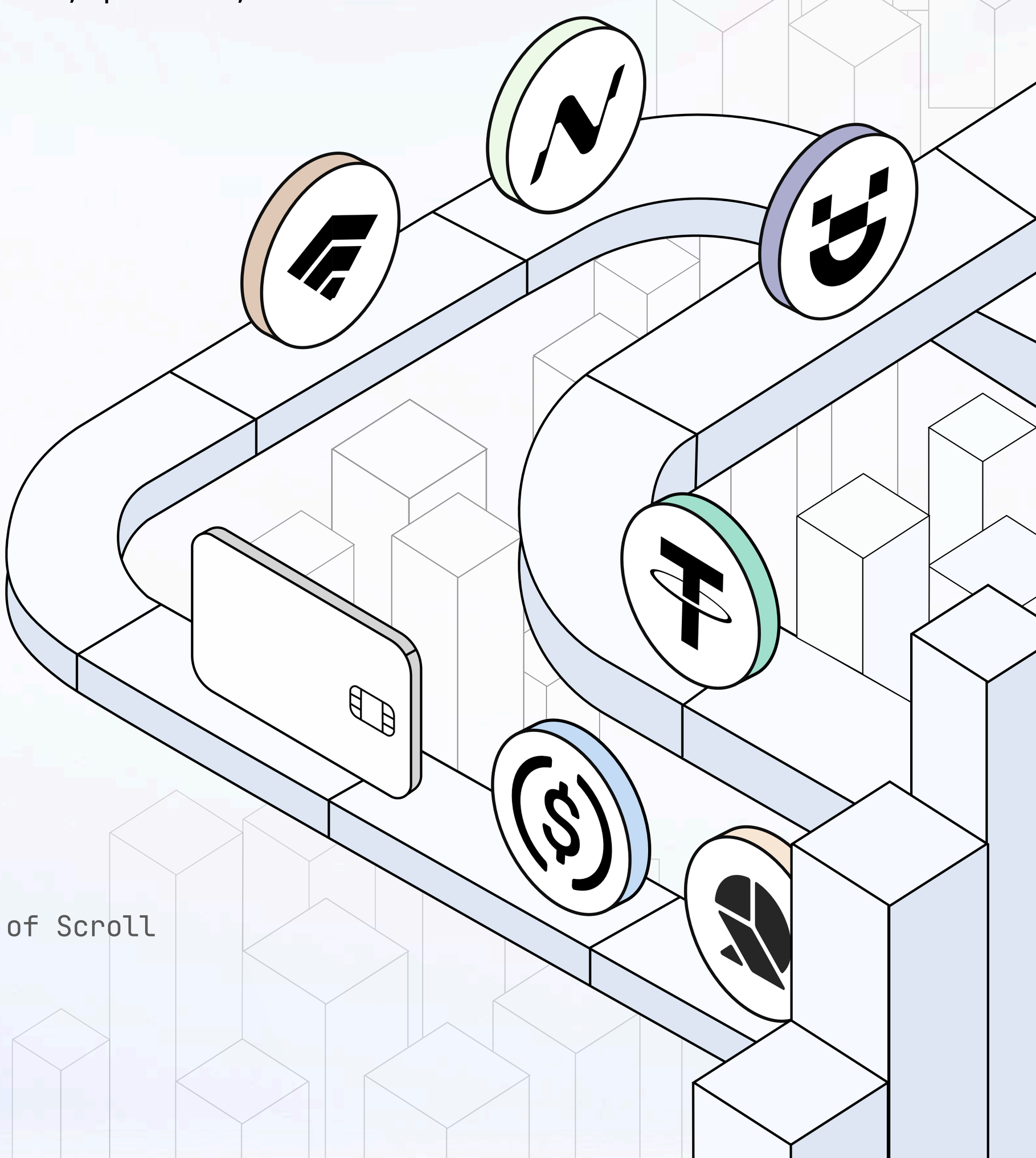
2025

The Stablecoin Story

Giants, yield, and the new trilemma:

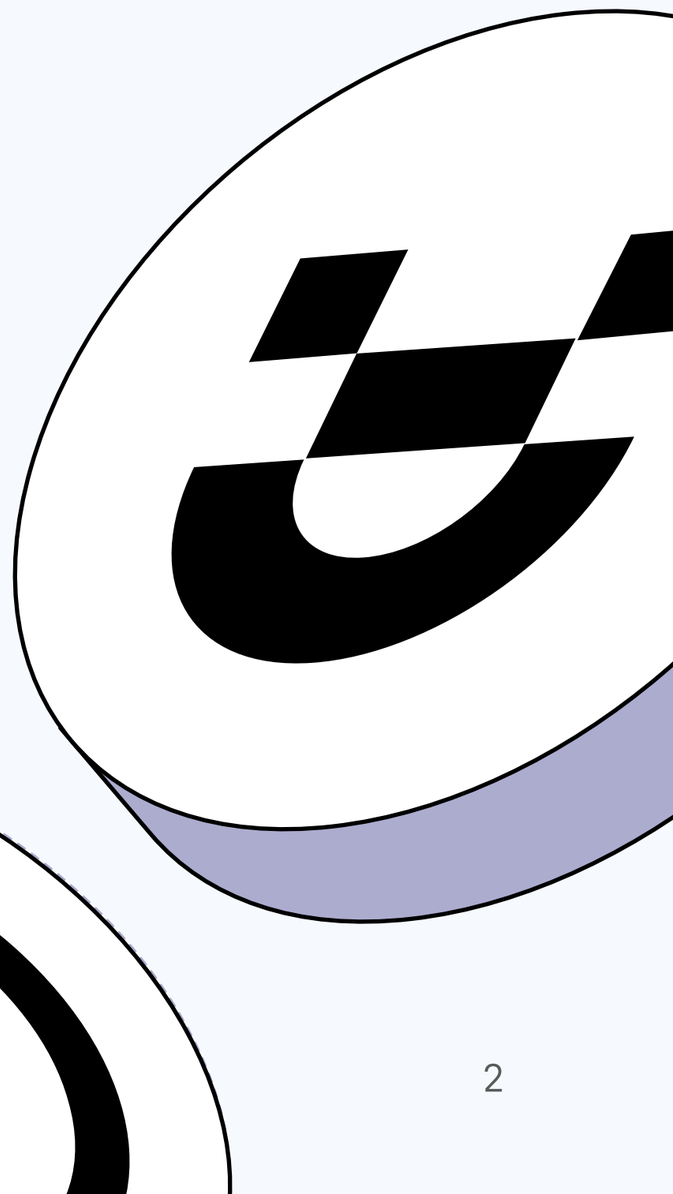
Breaking down the past, present, and future of digital money.



Sandy Peng

Co-Founder and CEO of Scroll

Table of Contents



Chapter 1: Introduction

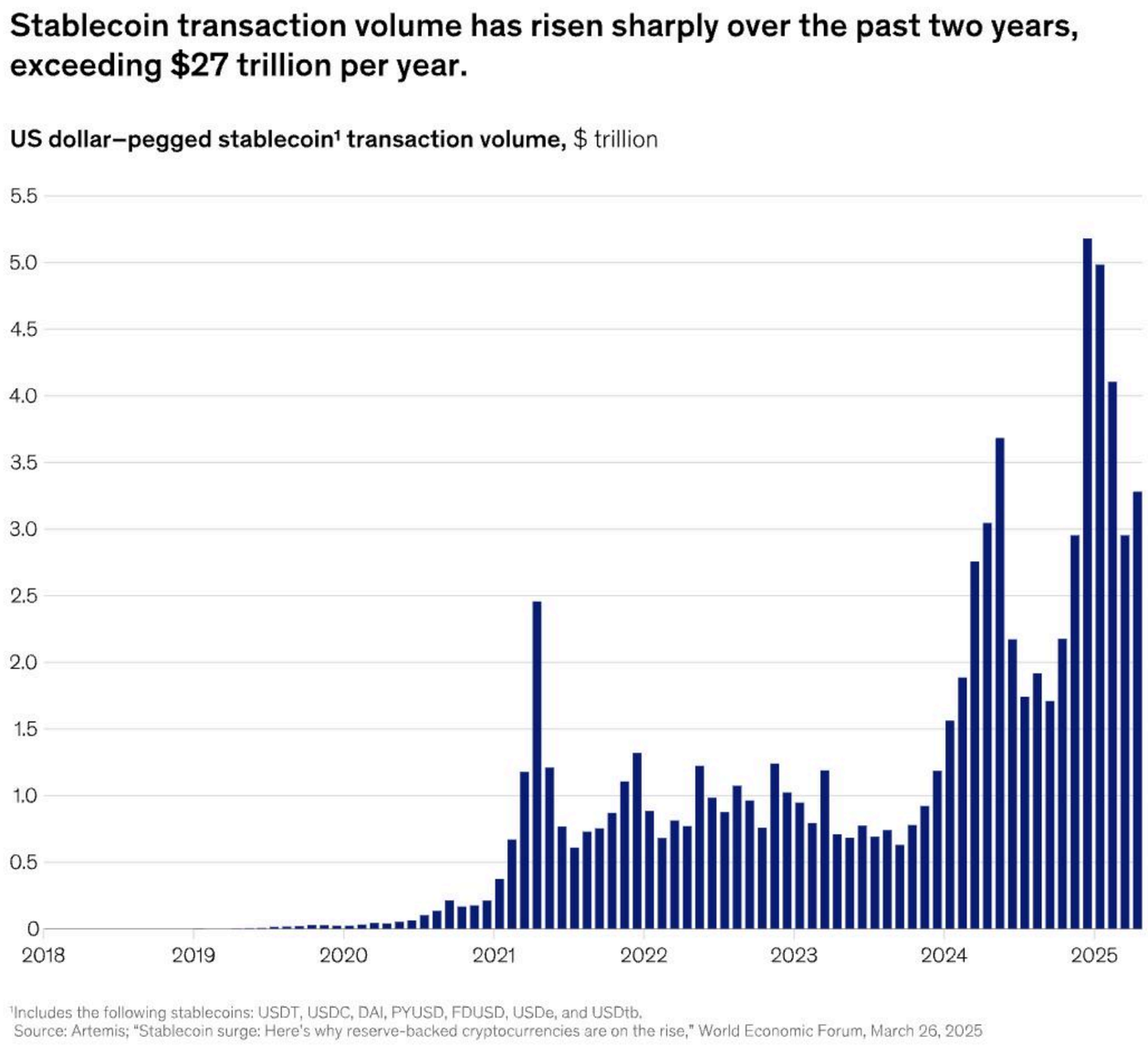
Most people tracking stablecoins can recite the numbers: $300 billion in supply, transaction volumes surpassing Visa and Mastercard, regulatory frameworks finally landing in the U.S. and Asia. The headlines always focus on the growth story. But growth stories are boring if you don't understand what caused them - and more importantly, what could accelerate or stall them next. The goal of this report is not to celebrate how big stablecoins got, but to understand the forces that lead to their initial success, the problems they solved, the limitations they hit, and the specific gap that's keeping the next trillion dollars on the sidelines.

The $300B inflection point

Stablecoins have reached a new inflection point in 2025 - evolving from what seemed to initially be a niche crypto use case into a significant pillar that is now reshaping global finance. In just a few years, the digital tokens pegged to fiat value have exploded in usage and market size, forcing both investors and regulators to take notice (and action). The rapid rise of stablecoins is now changing how payments operate, sparking regulatory action worldwide, and opening new opportunities for innovation in the next decade, in the aim to make money work as it always should have.

Global growth drivers

By mid-2025 stablecoins have reached roughly $305B in market supply, dominated (~85%) by USDT and USDC (Tether’s USDT alone is ~$180B). Transaction volume is yet another metric people often look at, as stablecoins are now moving trillions per year. Data show ~$27.6T in transfers in 2024 - far above legacy payment networks.

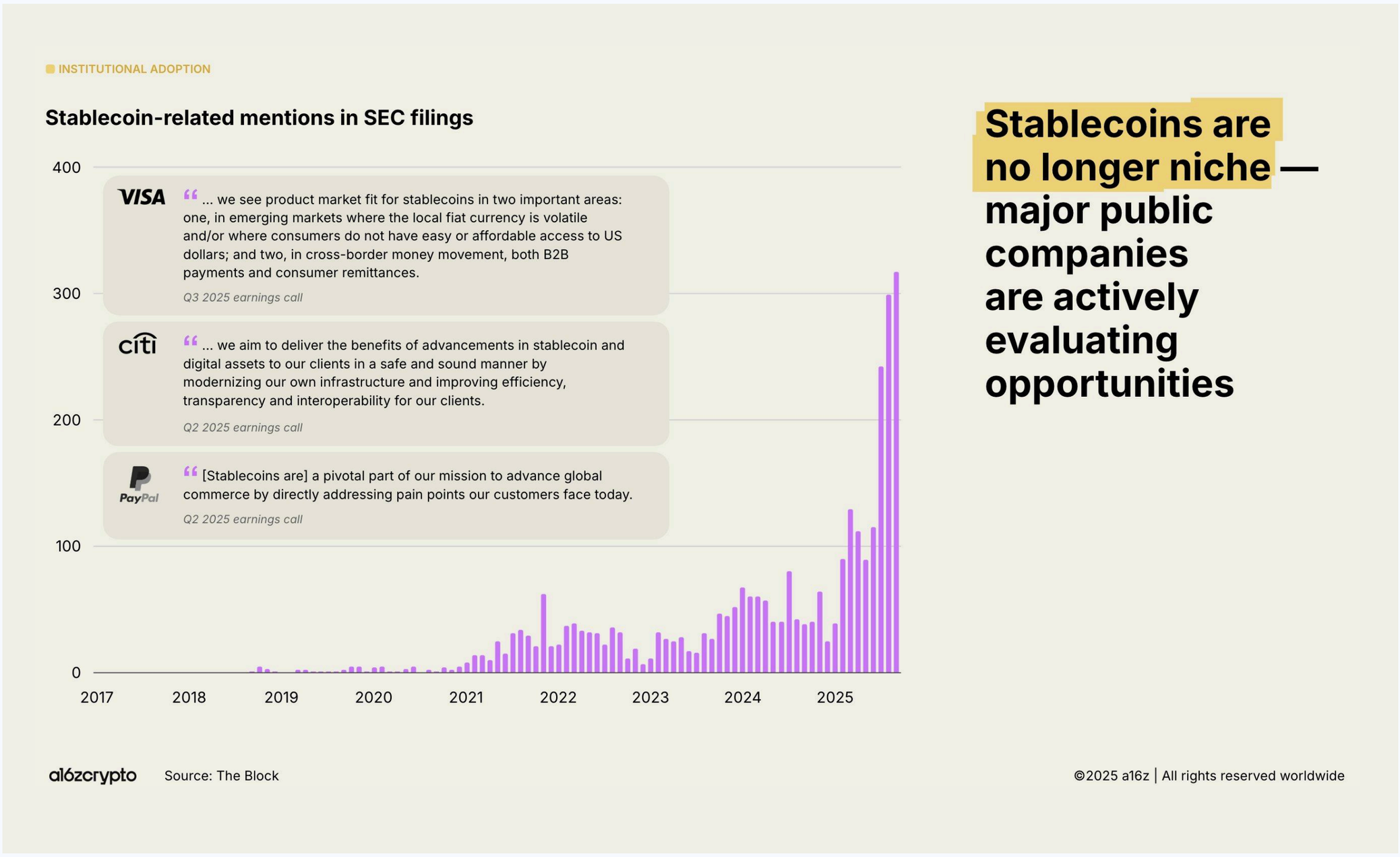


Source: Artemis via McKinsey

Emerging markets have driven much of this growth. In 2024, Latin America became one of the fastest-growing regions in the global crypto ecosystem, receiving a total of over $415 billion in crypto, with its global share rising from 7.3% to 9.1%, and the annual growth rate reaching 42%. Merchant and retail use is also rising, with many new crypto debit card solutions, as well as retail platforms accepting stablecoins, expanding use cases beyond trading.

In order to truly understand the motivations that led to this explosive growth, we also need to look at the series of global developments that fueled trust in stablecoins. This dramatic growth has triggered a wave of responses from policymakers and financial institutions around the world. In the United States, lawmakers moved to integrate stablecoins into the regulatory perimeter - the Senate passed the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act in mid-2025, establishing a federal framework for fully reserved “digital dollar” stablecoins.

Under the GENIUS Act, issuers must hold 100% USD reserves (e.g. short-term Treasuries) and abide by bank-like oversight, which is expected to catalyze broader adoption by legitimizing stablecoins within the traditional financial system. Across the Atlantic, the European Union's Markets in Crypto-Assets (MiCA) regulations (enforced starting 2023) set stringent standards on stablecoin reserves, supervision, and investor disclosures. Meanwhile in Asia, jurisdictions like Hong Kong and Singapore have crafted their own playbooks: Hong Kong's new "LEAP" framework consolidates all digital asset regulation under a single regulator and explicitly makes room for licensed stablecoin issuance and tokenized assets. This global patchwork of frameworks signals a common recognition that stablecoins are here to stay - and that clear rules are needed to harness their benefits while managing risks.



Source: a16z

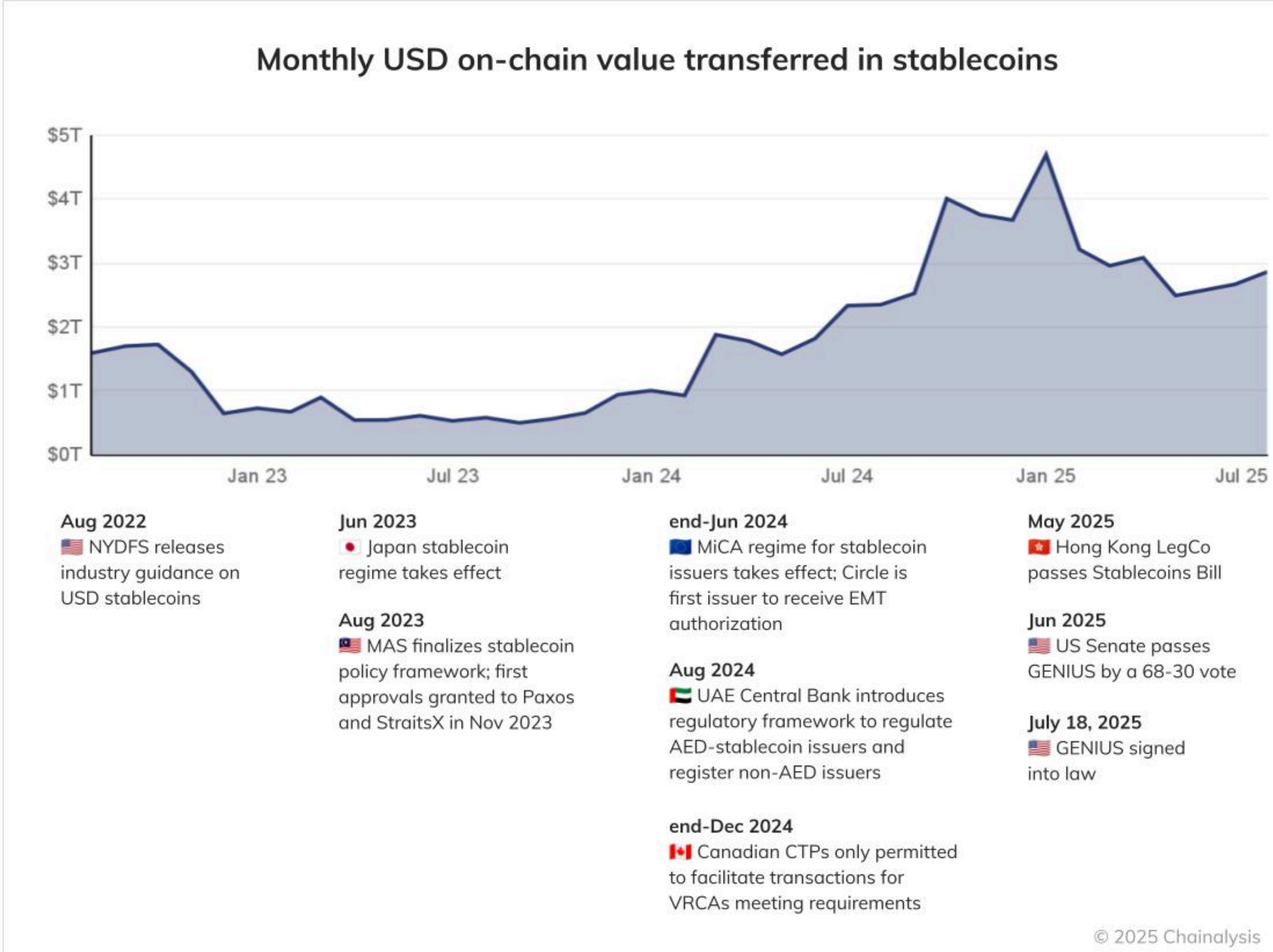
Three forces that broke the dam

For years, stablecoins lived in regulatory limbo - useful enough to scale, uncertain enough to keep serious institutions at arm's length. That changed in the later months of 2025, but not because of technology breakthroughs or viral adoption. The shift came from something more fundamental: legitimacy. Many governments around the world stopped treating stablecoins as crypto's weird experiment and started writing clear rules for how they should operate, the conversation moved from “should we?” to “how fast can we onboard?”. Institutions that couldn't get past compliance committees found pathways forward. The GENIUS Act and Hong Kong's LEAP framework didn't create demand - they removed the excuse not to act.

Then, treasury teams started running the numbers and realized traditional banking left significant yield on the table. A corporate finance team managing $50 million in operating reserves earns roughly $250,000 annually at 0.5% through a traditional bank deposit. That same capital deployed in stablecoin protocols with transparent reserve backing generates approximately $4 million at 8% APY - yield derived from U.S. Treasury bill rates, institutional DeFi lending spreads, and basis trading strategies on liquid derivatives markets. This reality prompted Web2 companies to reassess treasury strategies built for an era when better alternatives didn't exist. E-commerce platforms began holding settlement balances in USDC rather than waiting several business days for ACH transfers to clear. SaaS companies started parking monthly recurring revenue in yield-bearing stablecoins with instant redemption instead of money market funds that impose withdrawal restrictions. Payroll processors discovered they could capture yield on float - the window between when companies fund payroll and when employees receive payment - and use a portion of those returns as employee retention tools. The traditional banking model of capturing the spread between 0.5% deposit rates and 7% lending rates only functions when depositors lack viable alternatives. Stablecoins provided that alternative, and many treasury managers responded accordingly.

The last dam that contributed to the explosive growth was use cases expanding well beyond crypto-native trading activity. For years, stablecoin usage was concentrated in a single application: traders parking capital between positions to avoid volatility. That narrative no longer captures the scope of adoption.

In Q3 2025, retail activity strengthened significantly, with sub-$250 transfers reaching all-time highs in September and projected to exceed $60 billion by year-end. It is those small-value transactions that represent the shift - that stablecoins are now the new payment rails serving everyday economic activity. Stablecoins are now actively used across more than 50 countries, particularly in regions with high inflation or limited banking access such as Nigeria, Argentina, and Vietnam.

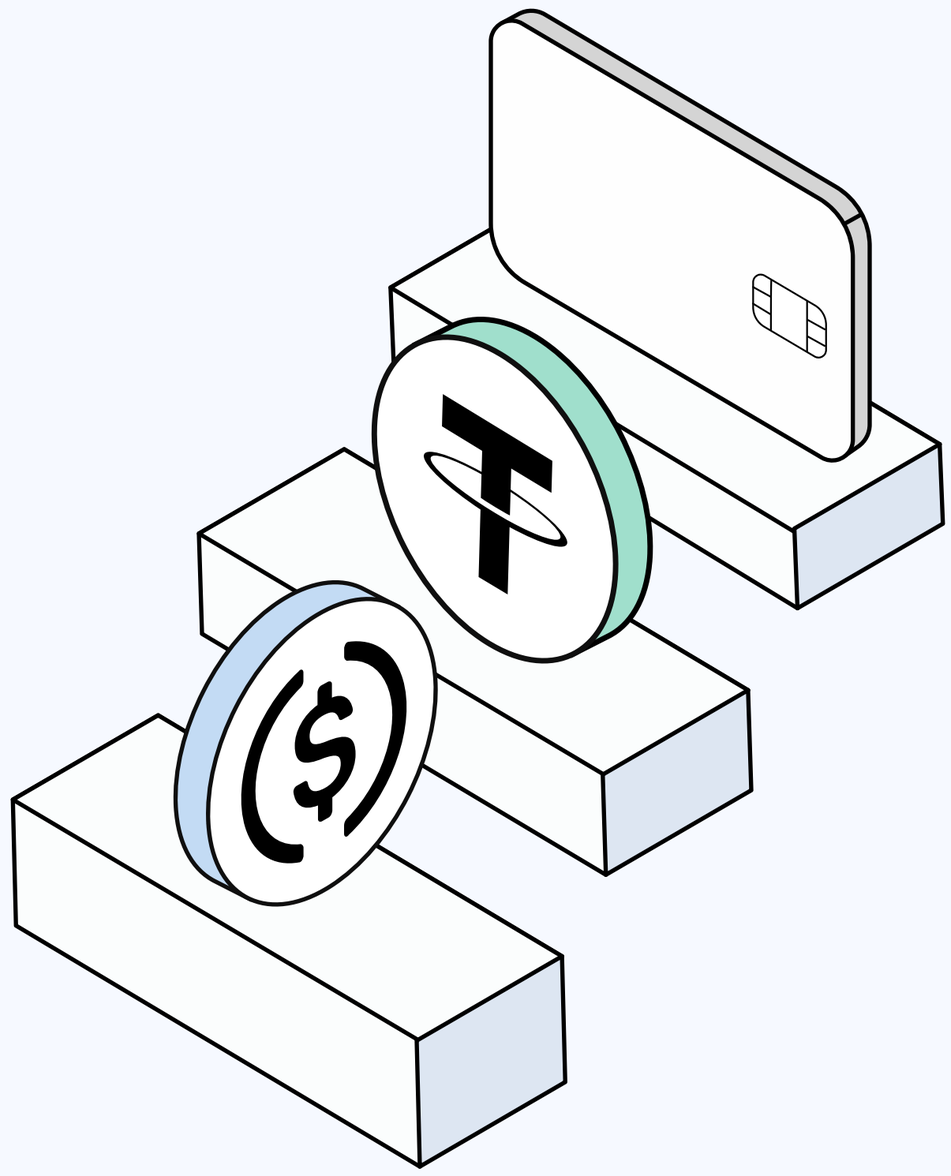


Source: Chainalysis

The cross-border payments sector demonstrates a similar story. Global remittances represent a $669 billion annual market with average fees of 6.65% per transaction - a tax on the world's most financially vulnerable populations. Stablecoins reduce those costs to basis points rather than percentage points while eliminating multi-day settlement windows entirely, and it’s clear that many countries adopted them as an alternative to their previous banking solutions.

The $2 trillion question nobody asked five years ago

Just five years ago, any stablecoin project seemed like a curiosity - now they hint at a multi-trillion-dollar future. JPMorgan recently noted that the current ~$305B market could reach $2 trillion under an optimistic scenario, generating an extra $1.4 trillion in U.S. dollar demand by 2027, whereas Standard Chartered sees a path to roughly $2T by 2028. In 2020 few envisioned stablecoins underpinning such volume; today even conservative forecasts treat a $3T+ stablecoin world as plausible. The real question now is how this will play out. If stablecoins truly become “programmable money” that powers global finance, their future impact could rival that of traditional banking infrastructure - a scenario we now urgently need to prepare for, even if it seemed inconceivable half a decade ago.



Chapter 2: Stablecoin giants and the new era of yield-bearing stablecoins

The rise of stablecoin giants (Gen 1 stablecoins)

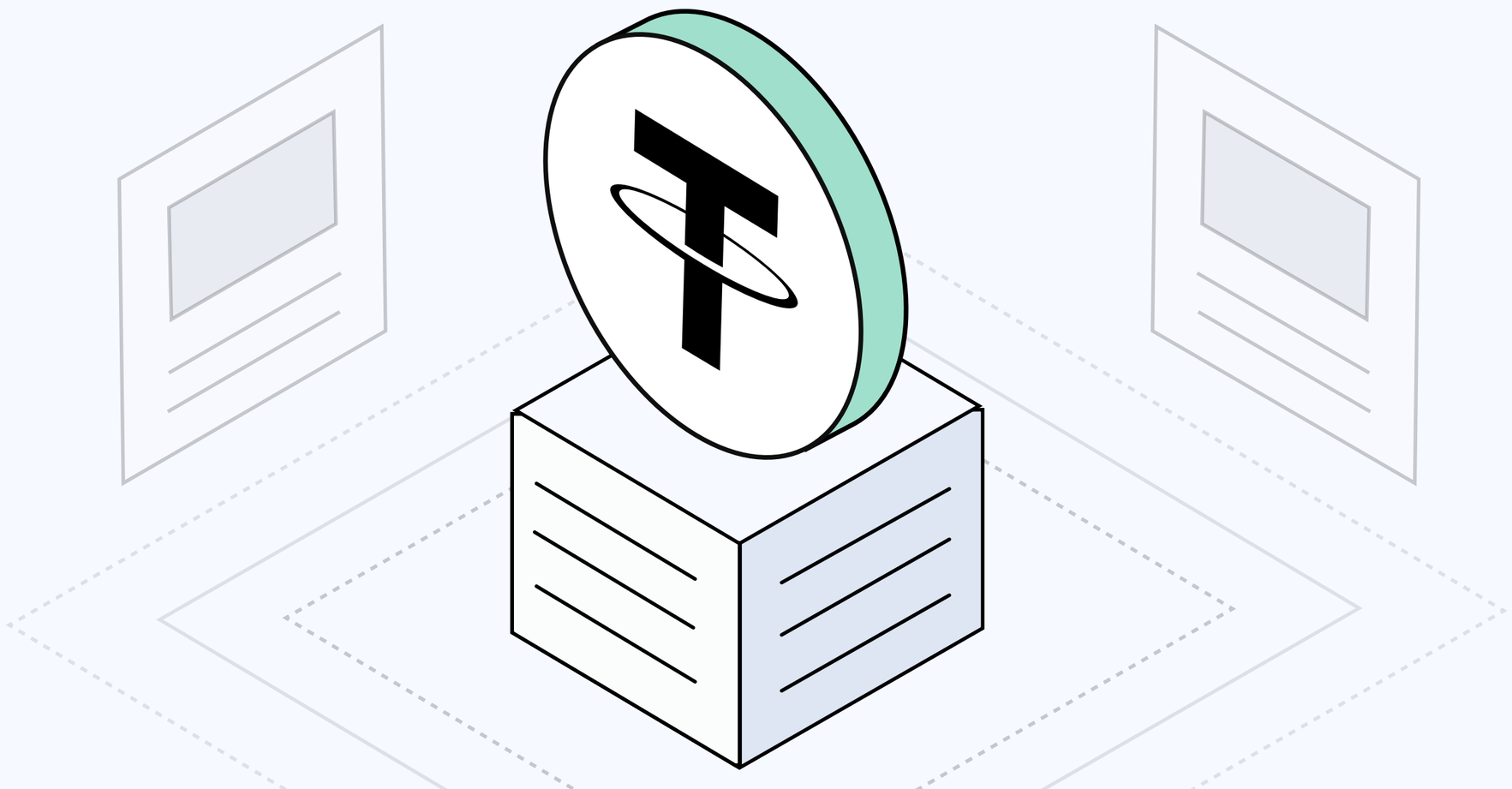
Tether (USDT) - From niche to COVID-era breakout

Since its inception, Tether’s journey has included pivotal moments that shaped its prominence. Initially, it didn’t look like Tether was going to win. When it launched in 2014, it was one of several stablecoin experiments - BitUSD and NuBits had already tried similar models. The difference is that Tether survived long enough to be in the right place when the world broke. It was March 2020 that changed everything for them - when COVID-19 lockdowns froze traditional banking infrastructure, when wire transfers stopped processing, and when currency exchanges closed their doors. Tether became the only financial rail that worked 24/7. Demand for digital dollars exploded. In mid-2020, USDT in circulation crossed $10 billion for the first time. By April 2021, that number had quintupled to $50 billion. The growth didn't stop. By late 2024, Tether's USDT reached a record supply of $139 billion. As of October 2025, USDT sits near $185 billion in circulation and has announced reaching 500 million users - roughly 6.25% of the global population.

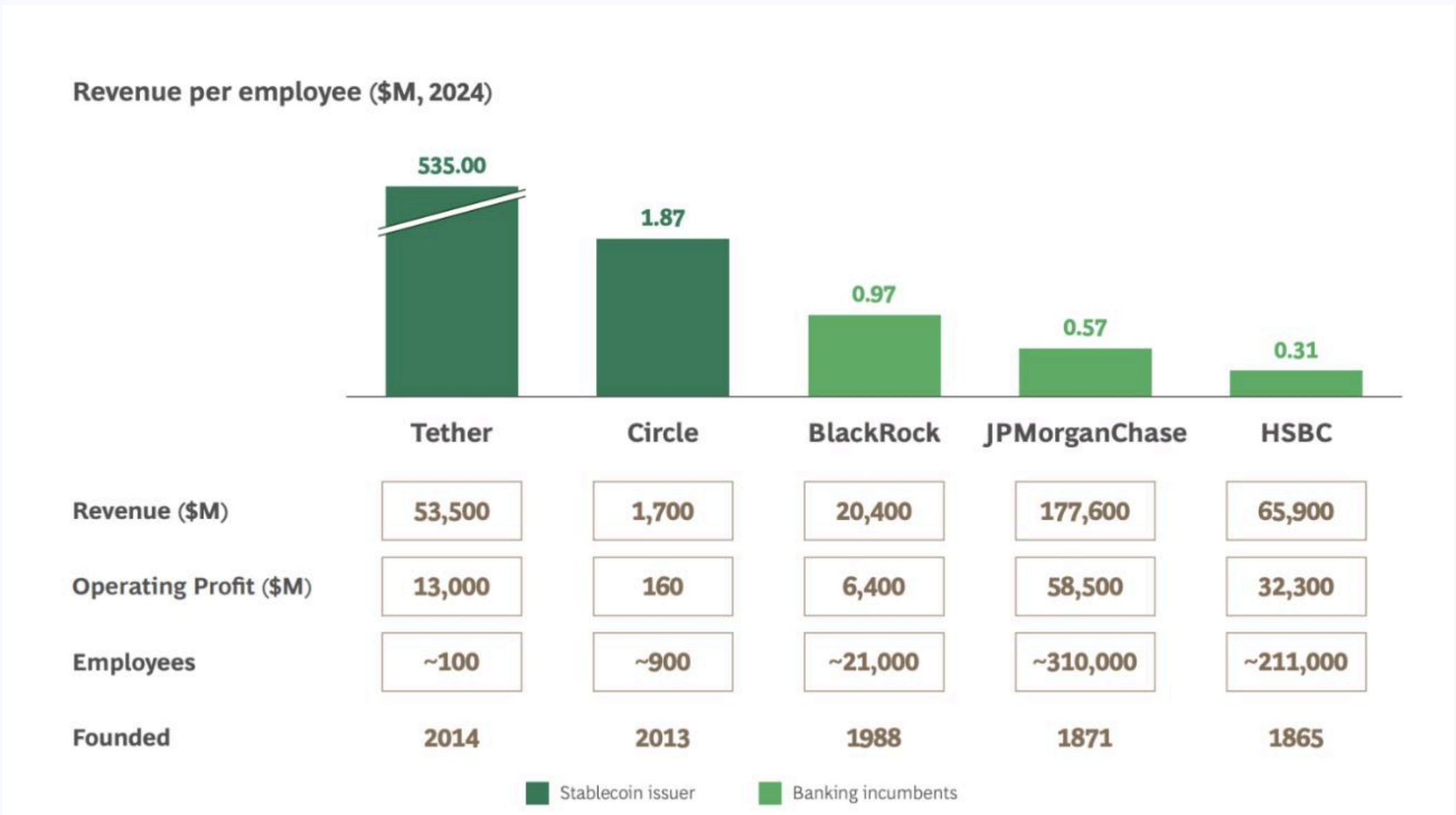
Tether is run by essentially the same team that operated Bitfinex - one of crypto's oldest exchanges. Paolo Ardoino, now Tether's CEO, has been with the organization since the early days. And this continuity clearly matters - while competitors cycled through leadership teams and pivoted strategies, Tether kept the same core group making decisions. It's the same crew, just with $185 billion more in responsibility and a user base that spans across most continents.

Tether now also holds the 18th largest U.S. Treasury position globally - larger than most countries. They also hold approximately 100 tons of physical gold. And massive Bitcoin reserves on top of that. Many would label this as a standard stablecoin reserve management - it’s more than that - they are building a doomsday vault. Paolo's thesis is straightforward: when traditional finance wobbles, when banks fail, when systems break - Tether becomes the lifeboat. Not because of technological superiority, but because their reserves are so diversified across asset classes and jurisdictions that traditional bank runs become structurally irrelevant. If the dollar weakens, they have gold. If governments freeze accounts, they have Bitcoin. If Treasury markets seize up, they have other liquid assets. It's a bet that the next financial crisis won't look like the last one, and having exposure to every possible safe haven means Tether can weather scenarios that would collapse single-asset-backed competitors.

Tether also happens to be one of the most profitable companies per employee in financial services. With a team of approximately 100 people, they generate billions in annual revenue - primarily from the spread between what they earn on reserves and what they pay out (which is zero, since USDT doesn't pay interest to holders).



Tether also happens to be one of the most profitable companies per employee in financial services. With a team of approximately 100 people, they generate billions in annual revenue - primarily from the spread between what they earn on reserves and what they pay out (which is zero, since USDT doesn't pay interest to holders).



Source: BCG report

Tether didn't win through better marketing or superior technology. They won by staying operational when alternatives failed, by building reserves that could survive multiple crisis scenarios simultaneously, and by maintaining leadership continuity while the rest of crypto churned through teams.

Circle (USDC): The institutional bet

Circle launched USDC in 2018 with a thesis that seemed naive at the time: regulatory compliance would eventually matter more than first-mover advantage. While Tether dominated with $20+ billion in circulation and network effects that seemed insurmountable, Circle built USDC around transparency, audited reserves, and relationships with regulators who could shut them down with a phone call. The bet was that institutions wouldn't touch stablecoins unless someone made them boring enough to pass compliance review.

USDC was designed to be fully reserved (backed 1:1 by cash or treasuries) and transparent - features that attracted institutions and fintech partners.

USDC’s growth started more gradually but picked up momentum alongside the DeFi boom. It reached its first $1 billion in circulation by mid-2020 and then exploded past $50 billion in early 2022. This swift rise reflected USDC becoming the stablecoin of choice for regulated businesses, traders, and decentralized finance applications seeking a trusted dollar token. Circle leaned into mainstream adoption, forging partnerships to bridge stablecoins with traditional payments. By 2025, USDC firmly held its position as the second-largest stablecoin, with roughly a quarter of the entire stablecoin market share. Circle’s strategy of proactive compliance and transparency proved prescient - when clearer regulations arrived, USDC was already aligned with the 1:1 reserve and disclosure requirements, which further boosted confidence.

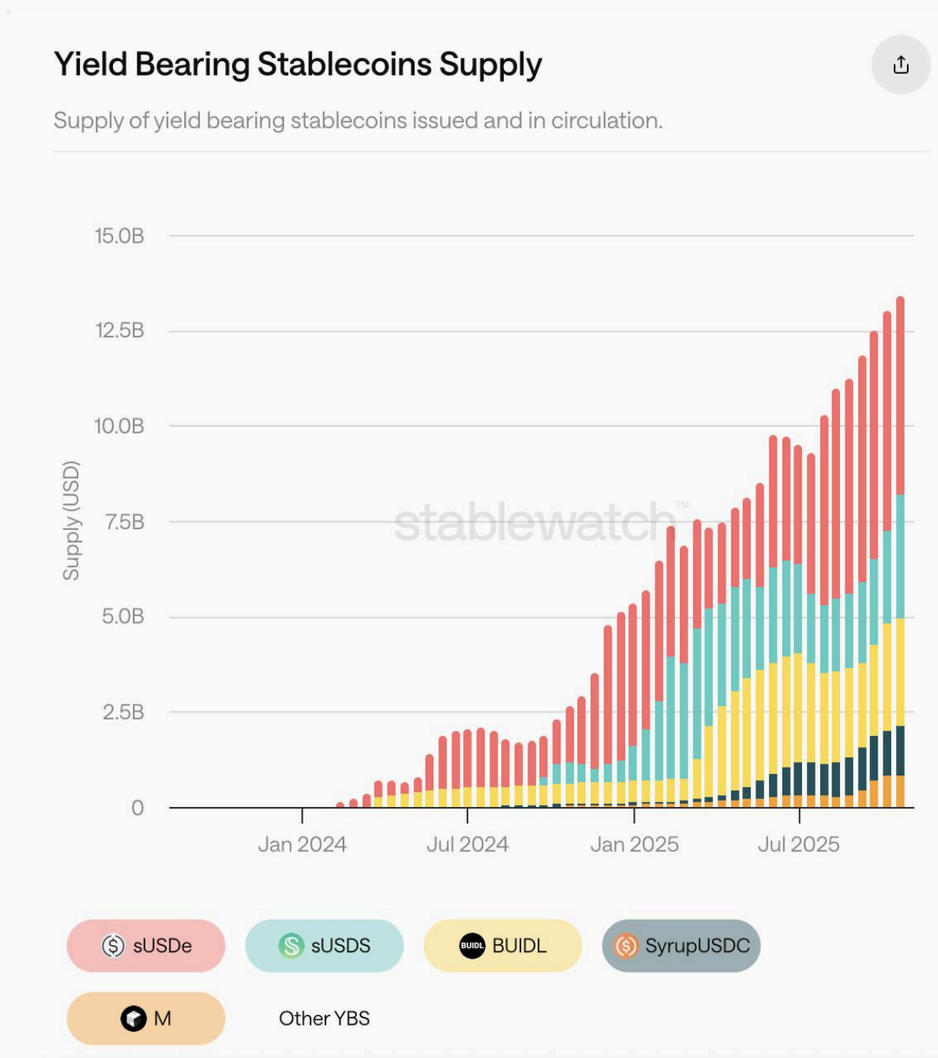
Circle's revenue model is also elegant. USDC holders receive zero interest, while Circle holds their reserves in U.S. Treasuries yielding 4-5%. With $75 billion in reserves, that's roughly $3-3.75 billion in annual interest income. In Q2 of 2025, Circle announced their total revenue and reserve income grew 53% year-over-year to $658 million. In June 2025, Circle went public. The IPO valued the company at just over $30 billion. For context, that's roughly half of Western Union's peak market cap, achieved by a company with a fraction of the employees and none of the physical infrastructure.

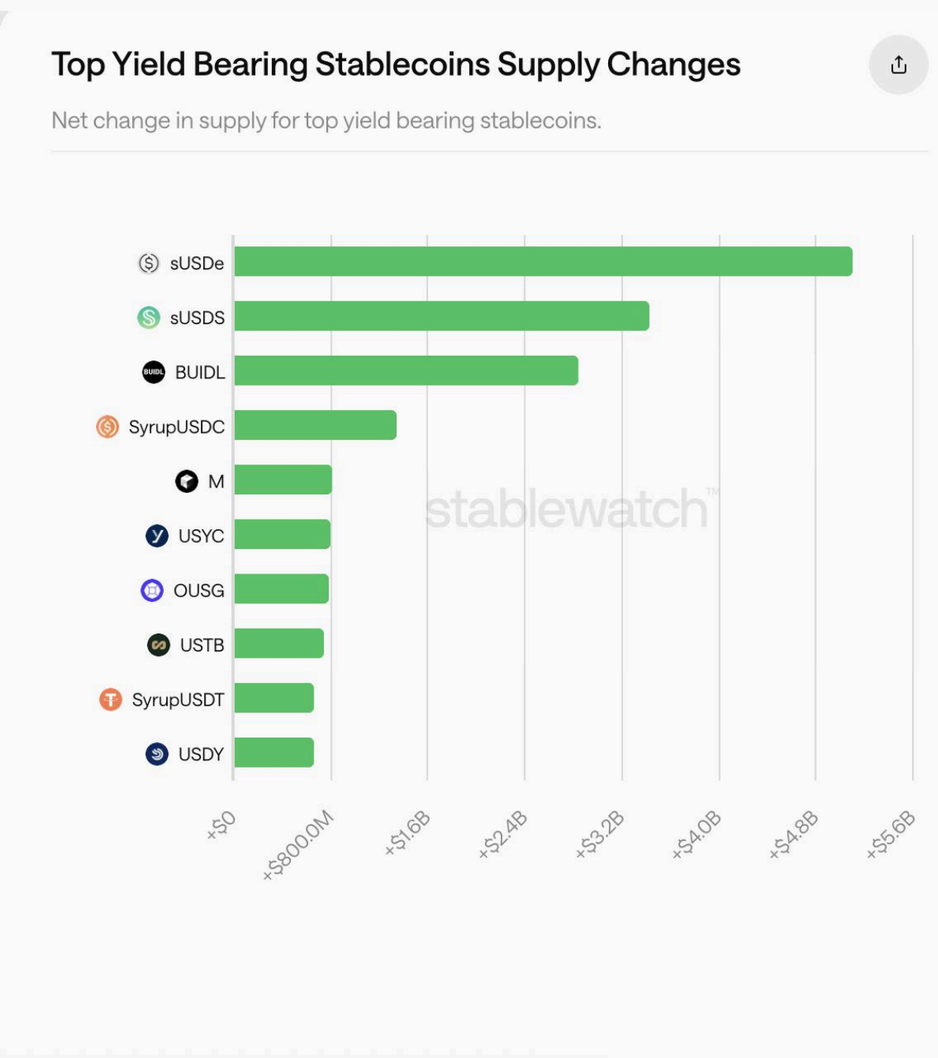
The pivot to yield-bearing stablecoins (Gen 2 stablecoins)

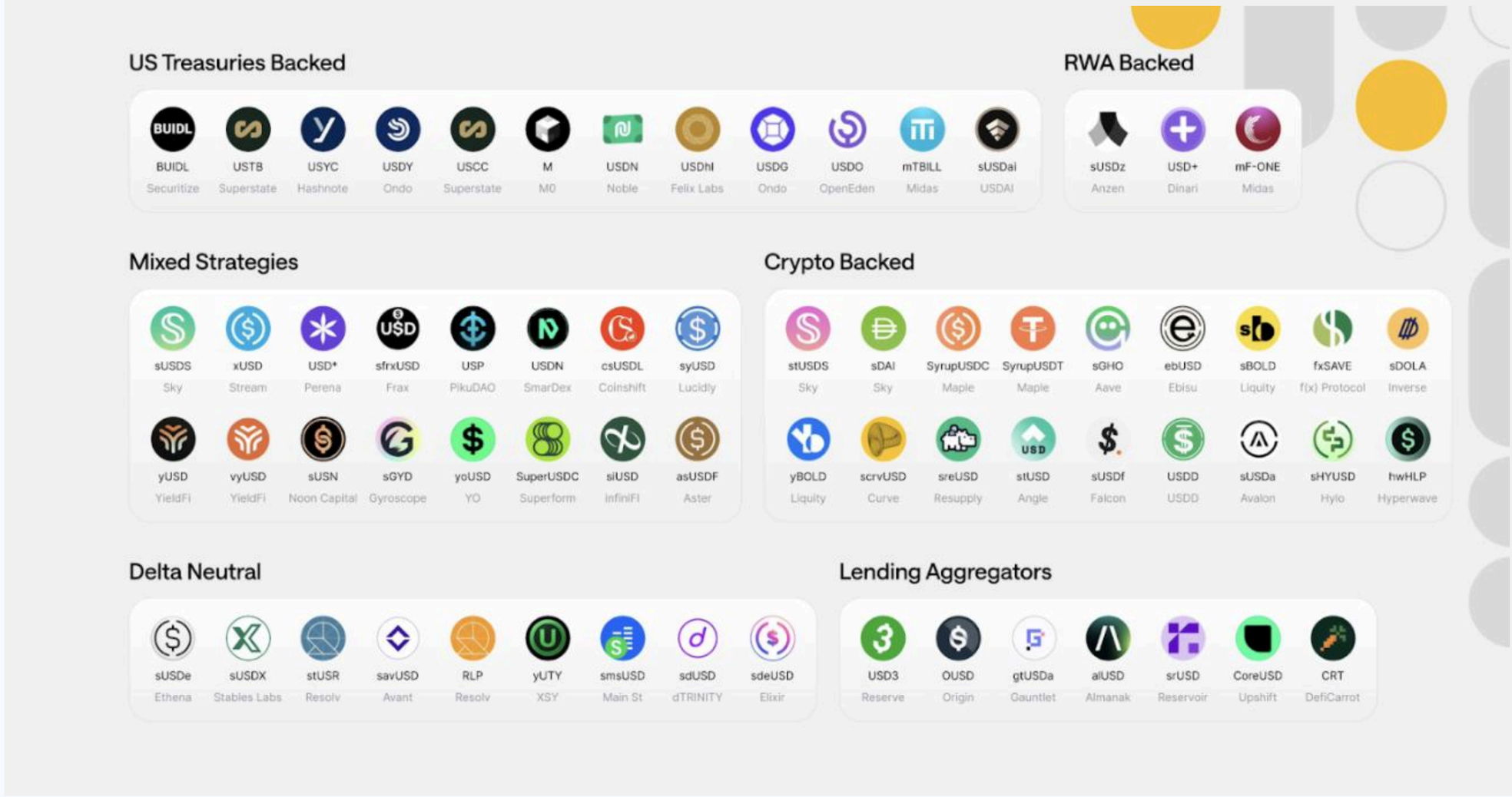
If gen-1 stablecoins gave us fast, borderless dollars, gen-2 stablecoins asked a different question: why should holding dollars onchain earn nothing when those same dollars could be generating 5-8% in T-bills or DeFi protocols?

The gap was obvious once anyone looked at it. Park $100,000 in USDC and earn zero. Park that same capital in a money market fund and earn $4,000-5,000 annually at prevailing Treasury rates. The difference wasn't a rounding error for businesses managing meaningful treasury balances or individuals holding six-figure stablecoin positions. It was enough to fund operations, cover payroll, or justify the entire cost of moving financial infrastructure onchain.

Yield-bearing stablecoins emerged to close that gap. They maintain the $1 peg that makes stablecoins useful for payments while generating returns that make them viable as treasury instruments. The category barely existed in early 2023. By mid-2025, yield-bearing stablecoins had grown from roughly $660 million to over $12 billion in market cap - a near-20x expansion in under two years.







Source: StableWatch

The growth is a clear trajectory - but the complexity is something many don’t understand. Keeping track of which protocols generate yield from where, how sustainable those rates are, and what risks come attached has become a full-time research exercise. New projects launch weekly, each claiming better rates or lower risk profiles than competitors.

Where the yield actually comes from

Yield doesn't materialize from nowhere. Gen-2 stablecoins tap into five primary revenue sources, each with different risk profiles and sustainability characteristics, explained on the next page:

1. **Lending pool wrappers** are the simplest model. Deposit USDC into Aave or Compound (or other lending app), receive a wrapped token like aUSDC that slowly accrues value as borrowers pay interest. The yield fluctuates with lending demand - when borrowing activity is high, rates rise; when demand drops, so do returns. It's straightforward, transparent, and fully onchain, but the yields are variable and usually sit in the 3-5% range.

2. **RWA-backed** stablecoins take a different approach. Protocols like Mountain Protocol's USDM or Ondo's USDY hold short-dated U.S. Treasuries and overnight repo as reserves, then pass the interest income through to token holders. The yields are more stable than DeFi lending rates because they're anchored to government securities, typically ranging from 4-5% depending on where the Fed sets rates. The trade-off is regulatory complexity - many RWA stablecoins require KYC, restrict access to accredited investors, or geofence certain jurisdictions entirely.

3. **Basis trading** stablecoins generate returns by exploiting the funding rate differential between spot and perpetual futures markets. Buy spot ETH, short an equivalent amount of ETH perps, capture the funding fees that leveraged traders pay. When funding rates are positive, this can generate 8-15% yields with theoretically zero directional exposure. The catch is that funding rates can flip negative, wiping out returns or even generating losses until the position is unwound and restructured.

4. **Protocol fee models** redirect trading revenue directly to holders. Curve's scrvUSD funnels borrowing fees and rebalancing charges from crvUSD into a reserve backing the yield-bearing version. Yield rises when protocol activity is high and falls when it's quiet. There's no external dependence on T-bill rates or CEX funding desks, but performance is entirely tied to whether users are actively borrowing and trading.

5. **Hybrid models** combine multiple sources. A protocol might hold 70% of reserves in Treasury-backed tokens for stability, allocate 20% to basis trading for higher returns, and deploy 10% in DeFi lending for additional yield. This diversification can smooth out volatility across any single strategy, but it also stacks risk exposures - custodian risk from the RWA side, exchange risk from the perps, smart contract risk from the lending protocols.

The world of possibilities keeps expanding. New protocols are launching with backing mechanisms that challenge assumptions about what can generate yield while holding a peg. Some tap into markets that didn't exist five years ago, others repurpose industrial infrastructure into financial primitives. Here are a few recent designs pushing the boundaries:

Plasma: Zero-Fee transfers fueled by internal incentives

Plasma is a purpose-built blockchain and stablecoin ecosystem (backed by Tether) that reimagines how a stablecoin network can reward users. Its flagship product Plasma One is a stablecoin-focused neobank that promises zero fees on USD₮ (USDT) transfers and a 10%+ APY on stablecoin deposits. How can it offer what sounds too good to be true? The answer lies in Plasma’s internal incentive model and architecture.

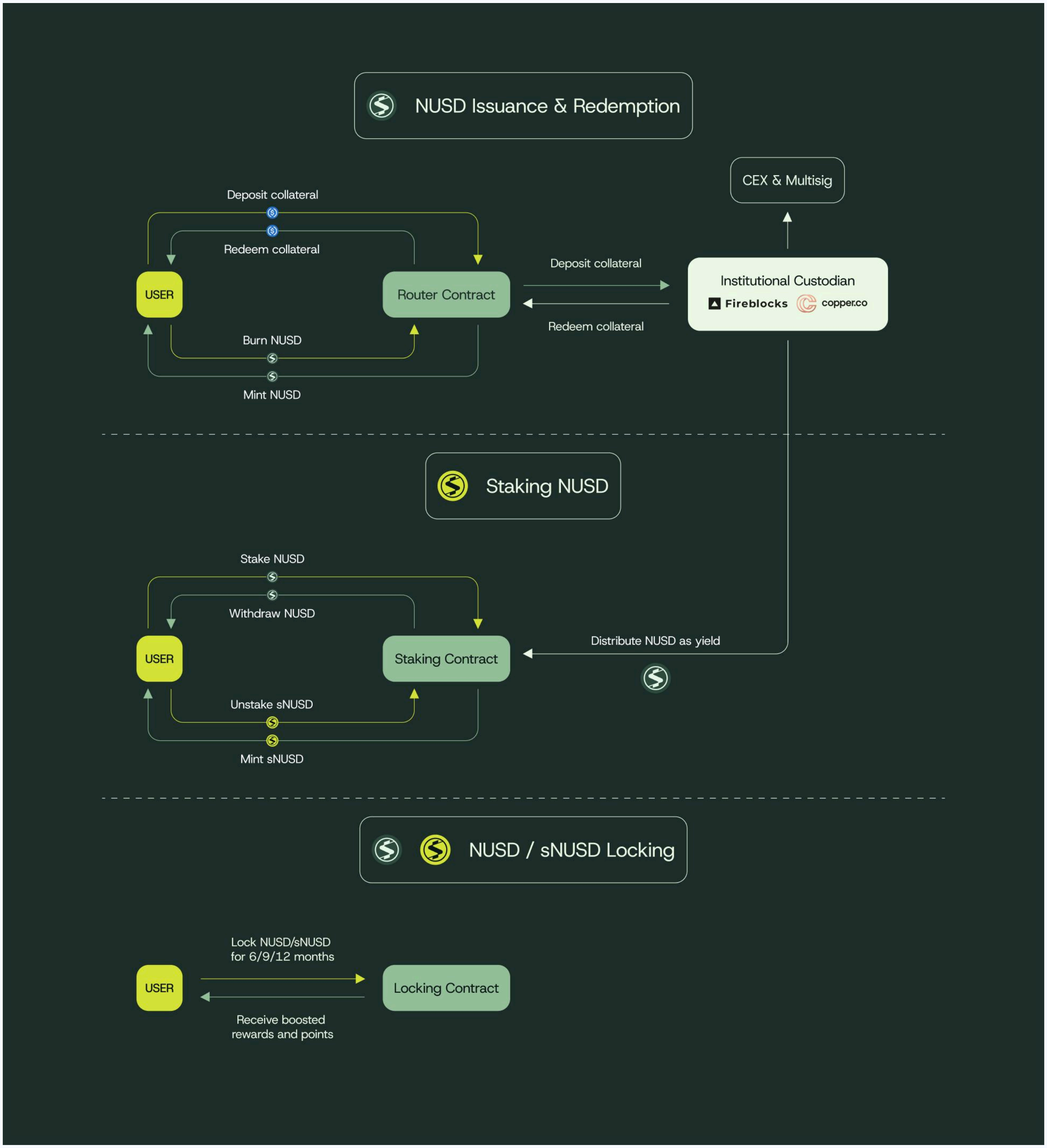
First, Plasma implemented an account abstraction “Paymaster” system to eliminate gas fees for end-users - effectively subsidizing transaction costs so that sending USDT incurs no fee. Those network costs are absorbed by the Plasma protocol itself, creating a seamless, feeless experience (crucial for micropayments, remittances, and everyday transactions).
Second, to fund its high yields and rewards (like 4% cashback on a stablecoin Visa card), Plasma acts as a yield aggregator behind the scenes. Its blockchain is EVM-compatible, letting it plug into 100+ DeFi protocols. Plasma then channels the yield from external DeFi strategies - e.g. earnings from lending markets, staking, and even other yield-bearing stablecoins like Ethena - back to its users. By tapping yields that far exceed the ~5% from Tether’s own reserves, Plasma can offer ~10% APY on USDT deposits with no lockup, effectively subsidized by DeFi revenue. In short, Plasma’s model is to reclaim value that was previously “given away” to other blockchains and protocols. Instead of Ethereum or Tron earning the fees and DeFi yields on USDT, Plasma’s network captures that value and returns it to USDT holders in the form of zero fees and interest. Plasma was one of the first chains to represent a shift toward vertical integration: the stablecoin issuer also runs the settlement layer and yield engine, aligning the entire stack to benefit the stablecoin users. It’s a bold bet that generous incentives and a dedicated L1 network can massively scale stablecoin adoption - essentially paying users to use stablecoins.

Neutrl: Market-neutral yield via arbitrage (NUSD stablecoin)

Neutrl is a DeFi protocol that introduced NUSD, a synthetic stablecoin engineered to generate high yield with minimal market risk. Its approach is to unlock sophisticated trading strategies - normally the domain of hedge funds - and package them into a stablecoin. Users mint NUSD by depositing traditional stablecoins (USDC, USDT, or even other synthetic dollars like USDe) into Neutrl, and in return receive an equivalent amount of NUSD.

What makes NUSD special is that when you stake it, you get sNUSD, a yield-bearing token that accrues the profit from Neutrl's underlying strategies. Those strategies are delta-neutral, meaning they aim to earn yield without directional exposure to crypto market swings. In practice, Neutrl runs a blended yield engine: the core strategy is arbitraging discounted OTC (over-the-counter) tokens - the team purchases future token unlocks from projects and early investors at deep discounts and hedges them. This is paired with onchain plays like basis trading and funding rate arbitrage on perpetual futures, all while keeping a portion in safe liquid assets. By combining these uncorrelated yields, Neutrl targets very high returns that are market-neutral. NUSD reportedly delivered around 30% APY on a $52 million pool (based on pre-deposits) - a testament to the untapped opportunities in OTC and derivative markets that Neutrl is tapping into.

The protocol emphasizes risk management (using vetted counterparties, legal agreements, and hedging every position) so that NUSD's $1 peg is maintained through a diversified collateral portfolio. Essentially, Neutrl is turning the esoteric world of OTC venture deals and perpetual swap funding into a simple stablecoin yield for users. This opens access for regular stablecoin holders to earn institutional-grade yields that were previously out of reach. As a delta-neutral stablecoin, NUSD represents the ethos of Gen-2 stablecoins: protect the downside (stay pegged to $1) while finding clever ways to earn yield on the upside. Neutrl is positioned to demonstrate how stablecoins can grow in value without sacrificing stability, by acting like a decentralized* (upon TGE) fund harvesting arbitrage opportunities round the clock.



Source: Neutrl documentation

Resolv: Two-token stablecoin with DeFi yields (USR stablecoin)

Resolv takes a unique two-tiered approach to create a yield-bearing stablecoin. At its core is USR, a stablecoin pegged to $1 and backed by a portfolio of onchain strategies. What sets Resolv apart is its dual-token architecture: USR is the senior stablecoin that is meant to be safe and stable, and then there is RLP, a junior risk token that absorbs volatility and enhances yield. This structure is reminiscent of tranching in traditional finance - users can choose to stake USR to receive allocation of Resolv collateral pool profits, while RLP holders take on the risk (and extra rewards) of the underlying strategies.

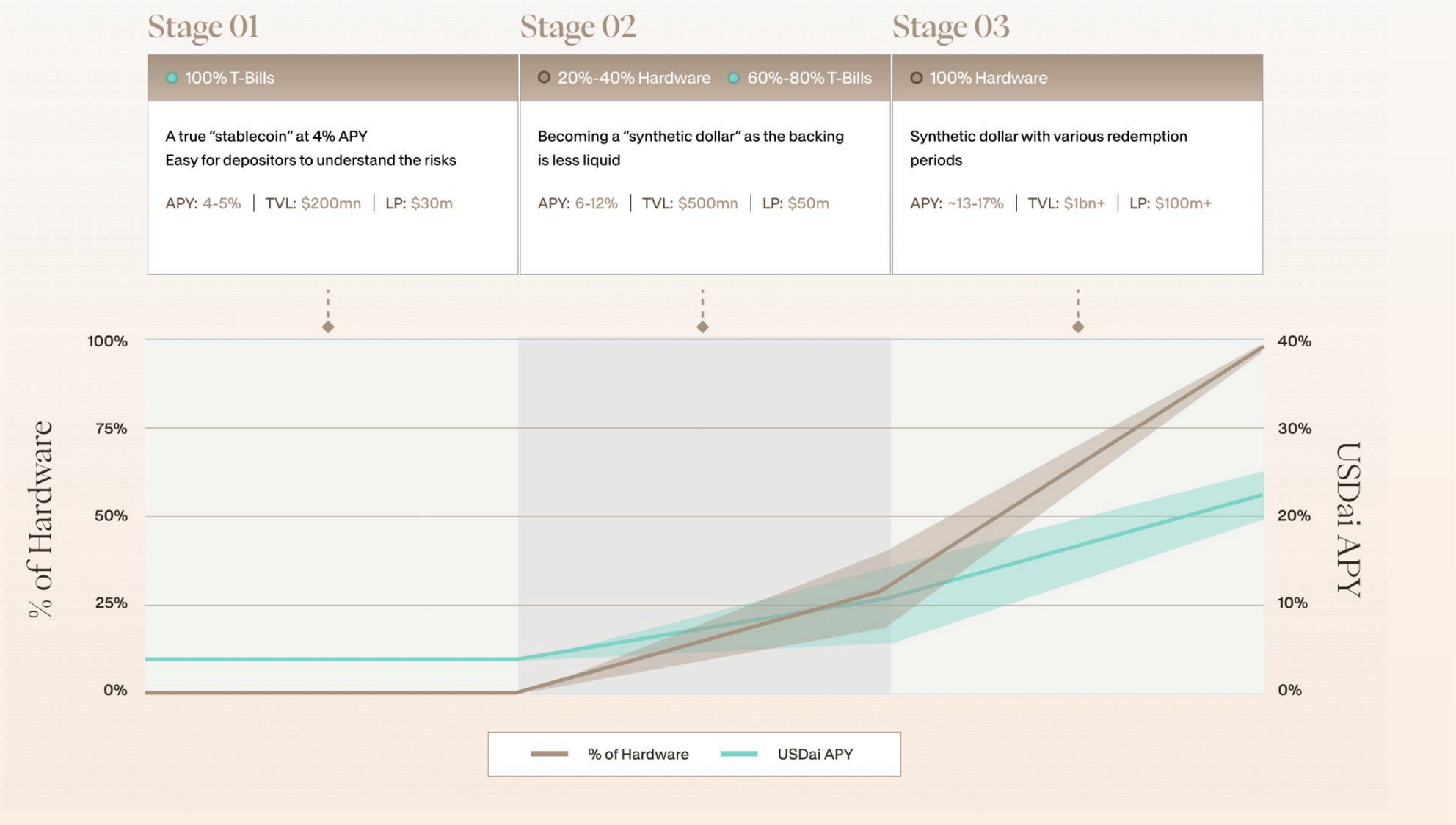
How does Resolv generate the yield feeding USR? It uses a delta-neutral investment strategy similar in spirit to Ethena's USDe approach, but with a different mix of sources. Resolv's treasury is collateralized by major crypto assets like ETH and BTC, but critically, it hedges away the price risk using perpetual futures or other derivatives. This means the protocol can earn base yields on assets (like ETH staking rewards) without being exposed to ETH's price fluctuations - the hedge keeps the net value stable. On top of that, Resolv pursues yields from multiple DeFi avenues: for example, it earns staking rewards from ETH/BTC, captures funding rate premiums on perp markets, and lends liquidity in DeFi lending markets. This modular yield design lets Resolv plug into whatever the best yields are in the crypto ecosystem while maintaining the peg.

Since launch in late 2024, Resolv has gained significant traction: over $390 million TVL and more than $1.7 billion in total USR minted/redeemed, distributing $10+ million in real yield to users. These figures show both the demand for yield-bearing stables and the effectiveness of Resolv's model. The two-token system is key to its resilience - USR holders have a "safe tranche" experience, whereas RLP holders act as a shock absorber (for instance, if any strategy underperforms, RLP takes the hit first). This allows USR to maintain stability even during turbulent markets. Backed by major crypto VCs, Resolv sees itself as "not just another stablecoin, but an infrastructure for investment-grade stablecoins". By isolating risk and automating complex yield strategies, Resolv's USR gives users an accessible stablecoin that earns passive income from the best of DeFi.

USD.AI: Stablecoin powered by compute (GPU-backed yield)

USD.AI is a project based on a fresh concept - which merges the worlds of stablecoins and artificial intelligence. The idea: use revenue-generating GPU infrastructure (the powerful hardware needed for AI model training and inference) to back a stablecoin and pay yield to stakers. In essence, compute power becomes the collateral and yield source for a dollar-pegged token. Developed by Permian Labs, USD.AI issues USDai, a $1-pegged stablecoin, and sUSDai, a yield-bearing version that accrues income from the underlying AI compute operations.

How does it work? USD.AI provides onchain loans to AI startups and companies, using their GPU hardware as collateral. These are businesses often starved of capital (AI hardware is expensive!), so USD.AI steps in to finance GPUs quickly, using stablecoin liquidity. The borrowers pay interest on these loans, and the GPUs produce AI services that generate cash flow - those income streams flow back into the protocol. This model “treats GPUs like commodities,” unlocking their value similarly to how oil or gold might back a financial product. For stablecoin holders, the appeal is that the yield is tied to the booming AI sector rather than crypto trading. Indeed, USD.AI’s pitch is that as demand for AI compute soars, USDai can “scale alongside global compute demands” and give investors a share of that growth in yield. Currently targeted yields are in the high single or low double digits - around 8% APY (with aims up to ~15%) for holding sUSDai. By August 2025, even before public launch, USD.AI had already attracted $50 million in deposits in a private beta and raised $13 million from major VCs to expand this GPU-backed lending model.



Source: USD.AI documentation

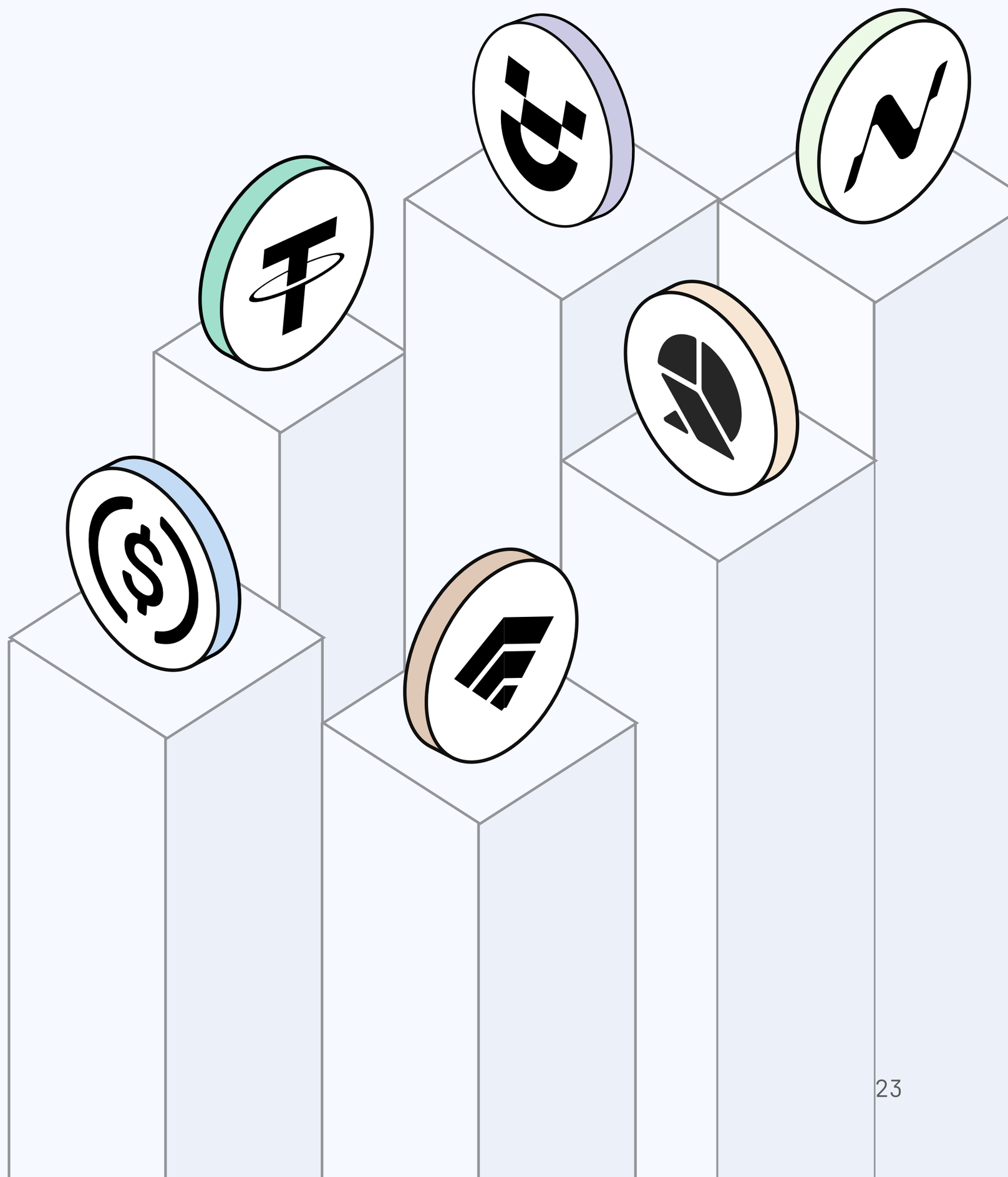
The broader vision is a convergence of trends: stablecoins becoming a vehicle for real-world asset yields, and AI's growth being funded by the crypto liquidity boom. USD.AI demonstrates this convergence vividly - every USDai token is essentially a claim on a portion of an AI data center's revenue. This "stablecoin meets AI" approach could create a virtuous cycle: AI firms get easier access to capital, and stablecoin holders get a yield "tied to AI sector growth" as Framework Ventures put it. It's a novel answer to the question of how to back a stablecoin beyond just fiat - by using one of the hottest commodities of the 2020s: computational power.

Daylight: Stablecoin yield backed by solar energy

Daylight is yet another interesting and novel use case, blending stablecoins with renewable energy. It's building a decentralized solar energy network, and at the heart of its model is DayFi - a stablecoin-like yield protocol linked to electricity revenues. The company installs solar and energy storage systems for homeowners with no upfront cost, and aggregates these home batteries into a virtual power plant. When the network sells electricity (for example, by supplying extra power to the grid during peak demand), the revenues from energy sales become the source of yield for investors in the DayFi stablecoin system. In other words, DayFi turns electricity into an investable, yield-generating asset. Users who hold/stake the DayFi stablecoin (details on the exact token name are forthcoming as the project evolves) will earn yield that is "tied directly to electricity revenues" from Daylight's distributed solar portfolio. This is a true real-world asset integration: yield is paid out from actual energy bills and grid service payments, not from trading or arbitrage.

The vision is powerful - as Daylight's solar network grows, more clean energy is produced and sold, and thus more revenue flows to token holders. It aligns the incentives of homeowners, investors, and the environment: homeowners save on energy costs and even earn Sun Points rewards, while investors earn a stable yield for financing the expansion of green infrastructure. Recently, Daylight raised $75 million from top VCs to scale this model. The DayFi stablecoin concept is a centerpiece of that plan, effectively opening the door for DeFi capital to participate in funding solar installations. By tokenizing energy income into a stable yield, Daylight creates a bridge between crypto and the physical world: you can invest stablecoins in something as tangible as electrons flowing through a solar grid, and get paid for it. This could accelerate renewable energy adoption by providing much-needed capital (via DeFi) and at the same time give stablecoin holders a new kind of yield backed by real assets (electricity). It's a prime example of the Gen-2 stablecoin ethos - innovate on the collateral and yield source. Instead of $1 in a bank account, one DayFi token might be backed by a dollar's worth of solar generation capacity. As this "electron-backed" stablecoin model matures, it could inspire a whole class of stablecoins funded by different real-world cash flows, from energy to commodities. Daylight is showing that even your power bill can be DeFi-fied, turning the utility of electricity into financial yield.

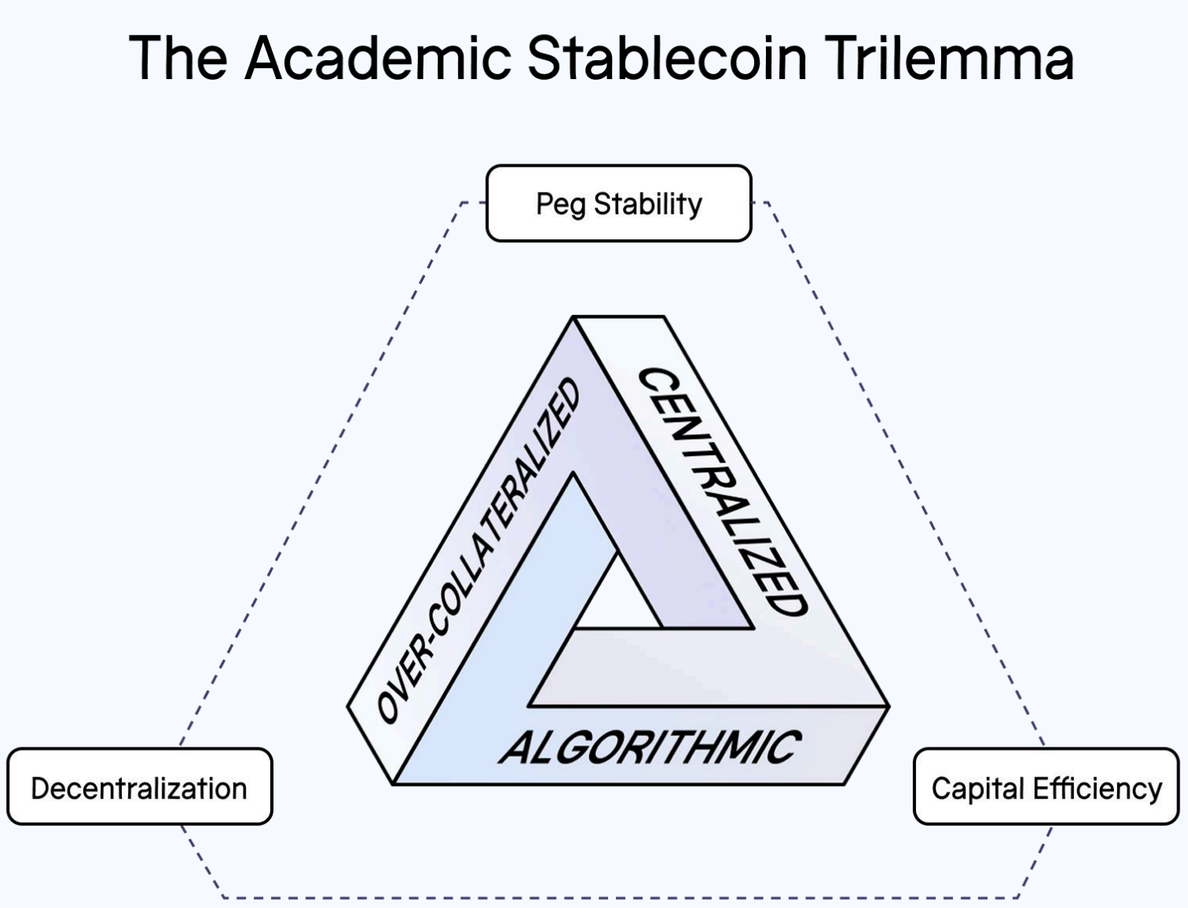
Crucially, these Gen-2 stablecoins still aim to maintain trust and peg stability (often with mechanisms to neutralize risk), but they transform a stablecoin from a static store of value into a productive asset. In doing so, they blur the line between savings accounts, investments, and digital cash. Users in the crypto ecosystem (and even outside of it) can hold a stablecoin that not only spares them from volatility, but also earns them a yield akin to a high-interest account or better - all while preserving liquidity and the ability to spend or transfer instantly.



Chapter 3: Rethinking the stablecoin trilemma

The traditional stablecoin trilemma (and why it’s incomplete)

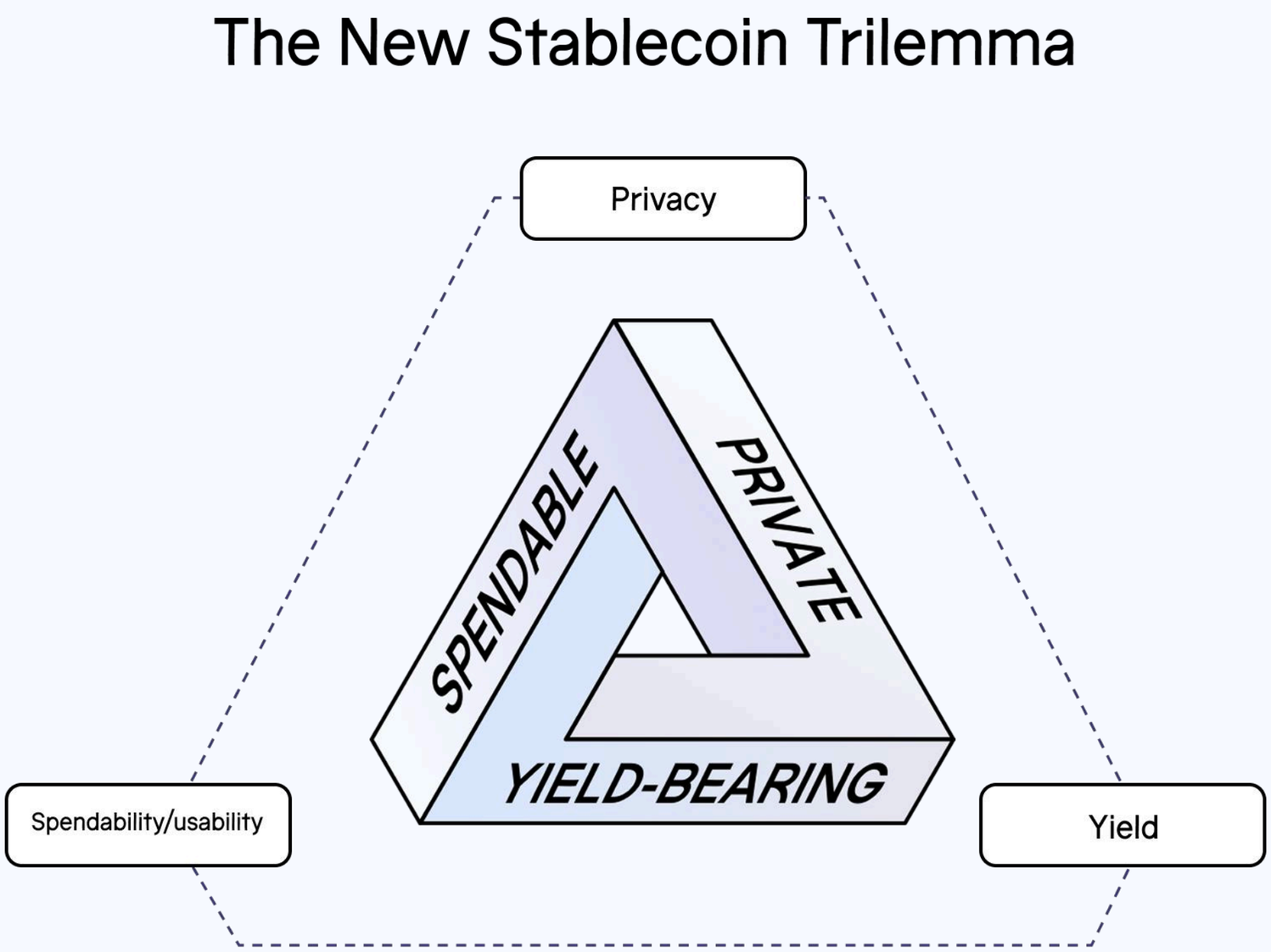
Cryptocurrency experts often talk about a stablecoin trilemma: the idea that no stablecoin can have all the ideal properties at once. In the classic view, the three coveted properties are price stability, decentralization, and capital efficiency. In simple terms, a stablecoin should maintain a steady value (stability), operate without central control (decentralization), and be efficient in how money is used to back it (capital efficiency). The academic argument is that a stablecoin project inevitably has to sacrifice one of these three goals. For example, a coin like USDC or USDT is very stable and capital-efficient (each token is fully backed by real dollars), but it’s run by centralized companies, not decentralized. On the flip side, a decentralized coin like DAI aims to avoid any single point of control, but it requires extra collateral onchain, meaning it isn’t very capital-efficient. This traditional trilemma frames the design challenges from a technical perspective.



However, focusing only on stability, decentralization, and capital efficiency misses a bigger point: Are stablecoins actually serving everyday users' needs? The classic trilemma is incomplete as it doesn't address the real-world experience of holding and using stablecoins. A coin could tick all the academic boxes and still flop if regular people find it inconvenient or risky to use. Solving the "textbook" trilemma doesn't guarantee a stablecoin that people will trust and adopt in their daily lives. We need to shift the perspective from the protocol's design trade-offs to the user's point of view.

The real stablecoin trilemma: Privacy, spendability, and yield

From a user-centric viewpoint, a truly useful stablecoin should excel in three areas that matter most to users: privacy, spendability, and yield. These form the real stablecoin trilemma - a trio of features that are rarely available all at once in today's stablecoins:



Privacy

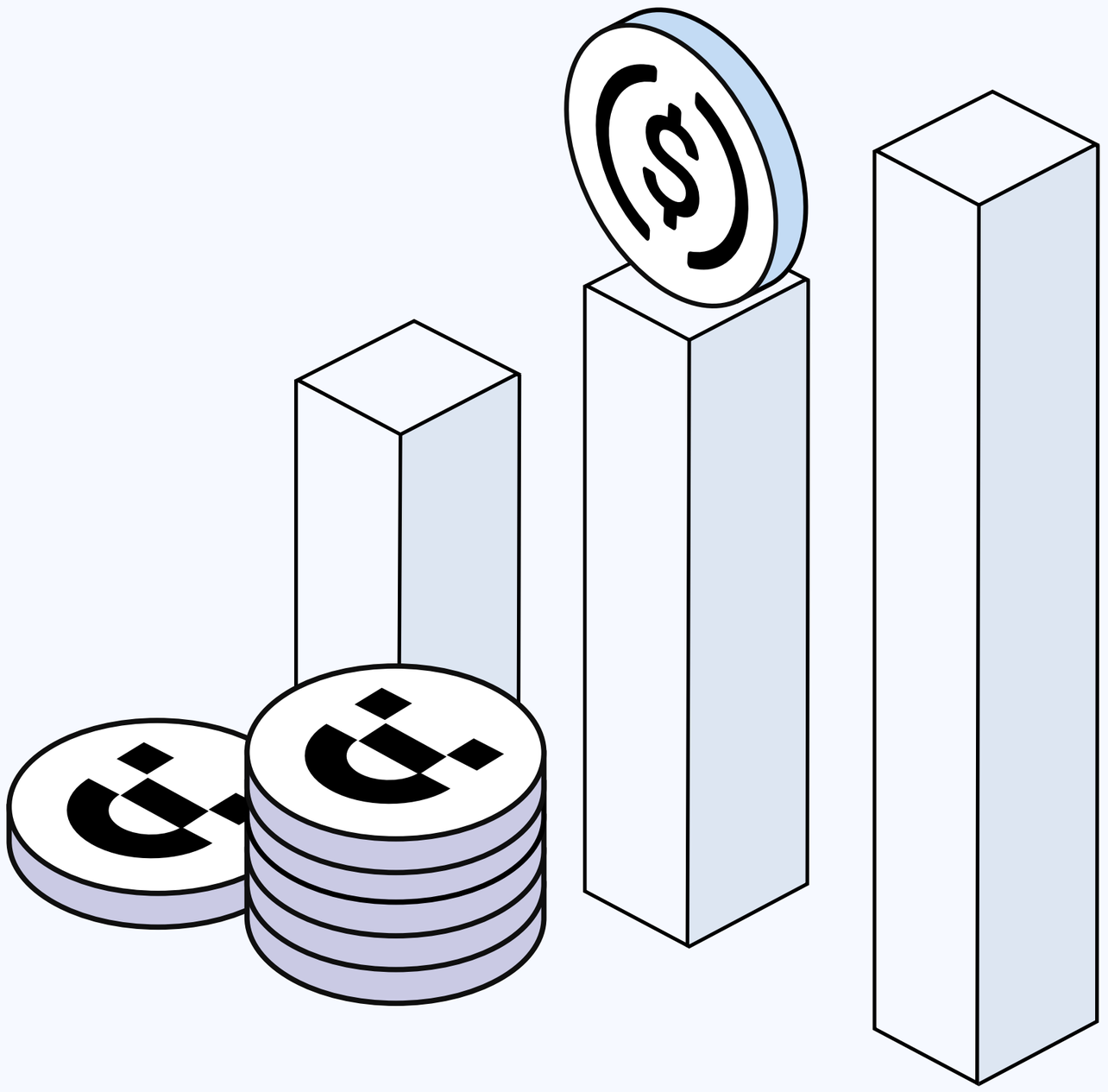
People want financial privacy, just like cash provides. Yet most stablecoins run on public blockchains where every transaction is traceable. If you send or spend a stablecoin, anyone can follow the trail by checking the blockchain. This lack of privacy has real consequences. For instance, when the U.S. government sanctioned an Ethereum mixing service, Tornado Cash, Circle (the issuer of USDC) froze over $75,000 worth of USDC linked to those. Users who care about confidentiality currently have to choose privacy-focused cryptocurrencies (like Monero) that aren't stable, since popular stablecoins don't yet offer built-in privacy. There's a clear gap for a stable-value coin that can be used without revealing your every payment or wallet balance to the rest of the world.

Spendability (everyday usability)

A stablecoin isn't very useful to ordinary people if you can't easily spend it for day-to-day needs. Today's top stablecoins were not originally designed for buying things in daily life. In fact, the early success of coins like USDC was driven by crypto traders using them to park value or trade in DeFi - not by people buying groceries. Even in countries where stablecoins became popular as a hedge against inflation (such as Argentina or Turkey), folks mostly treat them as a store of value - they convert local cash to USDT or USDC to hold savings, and then convert back when needed, rather than paying directly with stablecoins at shops. The user experience for spending stablecoins has been clunky: you often need to move coins to an exchange or bank to turn them into local currency, or find a merchant who explicitly accepts crypto. There have been some improvements recently, like special crypto debit cards that let you swipe your stablecoins. For example, the ether.fi Cash is being paired with a Visa card so that you can spend stablecoins anywhere Visa is accepted. Until now, using stablecoins in the real world required extra apps, cards or conversion steps. An ideal stablecoin should be as easy to use as cash or a debit card, without needing complex detours.

Yield (interest for holders)

One big question for anyone holding a stablecoin is, “what do I earn by holding this, compared to just keeping money in the bank?” Traditional money in a savings account can earn low-level interest - yet most stablecoins today don’t pay any interest or dividends just for holding them. In fact, regulations in some regions explicitly forbid stablecoin issuers from offering interest to holders. This means if you want your stablecoins to earn yield, you have to lend them out or use DeFi protocols - steps that are often too technical or risky for average users. While advanced users can chase yields by supplying stablecoins to lending platforms or liquidity pools, this is not straightforward or safe enough for the general public. The result: there’s a yield gap. People might be hesitant to keep large amounts in a stablecoin long-term because it just sits there doing nothing, whereas in a bank or money market fund it could be earning a return. A user-friendly stablecoin would ideally offer a built-in, low-risk yield or reward for holding it, making it a more attractive alternative to fiat savings.



Market gaps and unmet needs

No existing stablecoin fully satisfies all three of these user-centric needs at once, and that’s the core market gap. We have stablecoins that are stable and liquid, but they’re not private and don’t reward you for holding them. We also have some decentralized or interest-bearing stablecoin setups, but those often compromise on ease of use or broad acceptance.

In practice, users are forced to choose which feature matters most to them, and compromise on the others:

- If you choose a major coin like USDT/USDC, you get a reliable stable value and widespread exchange support - but every transaction is public and you earn zero interest on your balance.

- If you try a decentralized coin or DeFi solution to earn yield on a stablecoin, you might gain some interest, but you’ll face a more complex user experience and still have all transactions visible onchain. You also won’t be able to spend it at most shops directly.

- If you insist on financial privacy, you’re likely using a privacy coin or cash - and neither of those gives you a stable price and the benefits of crypto finance at the same time.

These trade-offs highlight a real opportunity for innovation. The first generation of stablecoins hasn’t delivered that combination yet. Even as stablecoins grow into a huge industry, this user-centric trilemma remains a huge question, and a new problem to solve for.

Chapter 4: Solving the stablecoin trilemma - Privacy, spendability, and yield in practice

Real users, real trade-offs in emerging markets

Many emerging markets face a perfect storm of economic challenges: high inflation, unstable currencies, and limited access to traditional banking services. Stablecoins promise to be the alternative - digital cash that’s as private as paper money, as spendable as a bank card, and even yield-bearing like an investment. In reality, everyday users often face a trade-off - they can rarely get all three qualities at once. As the previous chapter outlined, the new “stablecoin trilemma” is playing out on the streets of many emerging markets, where demand for stablecoins is high but user experience gaps are evident.

One such example is Africa, which should be a stablecoin success story by now - the continent has volatile local currencies, limited banking access, ubiquitous mobile money, and a young, tech-savvy population hungry for alternatives. Yet even in Nigeria and Kenya, where crypto adoption leads the continent, stablecoin usage remains niche outside early adopters. During a recent team visit to Lagos and Nairobi, we have observed firsthand how these trade-offs and frictions are stalling broader adoption despite the clear need and enthusiasm.

Below are the top 10 African countries with the highest crypto ownership:

Rank	Country	Crypto ownership
1	South Africa	10.0%
2	Nigeria	5.9%
3	Kenya	5.1%
4	Egypt	3.0%
5	Tanzania	2.4%

Source: Business Insider Africa

The demand signal is unmistakable. Nigeria ranks among the top countries globally for crypto adoption, with stablecoins actively used as a hedge against the Naira's volatility. Kenya's M-Pesa has 30 million active users moving over $300 billion annually through mobile money - proving the infrastructure and user behavior for digital payments already exists at massive scale. The population skews young, with median ages in the mid-20s, and smartphone penetration continues climbing past 50% in urban centers. With unstable local currencies, and traditional banking serving less than half the population, the conditions for stablecoin adoption couldn't be more favorable.

Yet growth remains constrained by the same problems plaguing stablecoins everywhere, only amplified. Public transaction visibility becomes dangerous when showing dollar holdings can make someone a target in cash-dependent economies. Zero yield means stablecoins compete poorly against local savings mechanisms that offer returns, even if denominated in depreciating currency.

Clunky user experiences requiring gas fees, wallet management, and blockchain literacy create friction that mobile money platforms solved a decade ago.

Solving the real stablecoin trilemma - privacy, spendability, and yield - unlocks these markets in ways gen-1 and gen-2 stablecoins cannot. Private transactions mean holding dollars doesn't broadcast wealth. Seamless spendability means stablecoins work as intuitively as M-Pesa, not crypto infrastructure. Sustainable yield means users earn returns that compensate for adoption risk and learning curves. Get all three right, and the addressable market isn't millions of early adopters - it's hundreds of millions of people who already use mobile money and would switch to better rails if those rails actually worked better across every dimension that matters.

Privacy vs. trust: The informal workaround

In many emerging regions, privacy is more than a preference - it’s protection. Regulatory uncertainty has been a big wild card, with abrupt policy shifts creating fear that holdings could be frozen or outlawed overnight. We found that many users, wary of crackdowns, avoid formal exchanges and resort to peer-to-peer channels to trade stablecoins. Going informal (direct P2P services), however, comes at a cost. Without regulated platforms as middlemen, users shoulder more risk - we heard stories of scams and deal disputes, and indeed wallet thefts and fraud are common concerns in these underground markets. Privacy is achieved (no KYC forms, no government IDs), but trust and safety are weaker, and it’s hardly scalable. Users want digital dollars they can use freely without surveillance, yet the very solutions that enable that freedom today also erode confidence and convenience.

Regulatory progress might eventually ease this tension - for example, Nigeria’s recent crypto framework signals a more open stance. But until rules stabilize and mainstream channels offer both compliance and privacy safeguards, many will remain stuck in the gray market. The paradox is clear: people crave privacy and control, but the lack of officially sanctioned private stablecoin options forces them into clunky workarounds. True adoption will require bridging this gap, finding a way to protect user privacy without keeping stablecoins on the fringe.

Spendability vs. friction: Stablecoins still aren’t plug-and-play

For a currency to go mainstream, you must be able to spend it easily. Here lies the second leg of the trilemma: stablecoins might be pegged to dollars, but using them for everyday transactions is still far from frictionless in many emerging markets. Every stablecoin purchase often involves an extra step - typically cashing out to mobile money or bank money - which adds time, fees, and hassle. Even tech-savvy freelancers who earn in stablecoins tend to “cash out only what they need” for immediate expenses, keeping the rest in digital dollars. This behavior highlights a key point: stablecoins excel at cross-border transfer, but stumble at the last mile. Converting in and out of fiat is still a pain point. Weak on/off ramps and low local liquidity often mean people pay a premium or wait hours to move between stablecoins and cash.

There are promising moves to improve spendability. In East Africa, services like Kotani Pay now let users receive a stablecoin and have it appear as M-Pesa balance, inside a familiar mobile wallet. Some fintech apps are even hiding crypto under the hood - Chipper Cash, for example, shuttles funds in USDC behind the scenes so that customers just see a faster, cheaper money transfer in their local currency. These integrations make stablecoins feel practically invisible and therefore usable, plugging into habits people already have. Still, such solutions are early. The potential is there - mobile money proved Africans embrace digital finance when it works seamlessly - but stablecoins must integrate with everyday commerce to cross the chasm. Right now, every extra step or confusing interface in the process is a point of friction that chips away at adoption.

Yield vs. simplicity: Missing incentives for savings

The third piece of the trilemma is yield - the idea that holding a stablecoin could earn you interest or rewards. For users in high-inflation economies, this is hugely attractive in theory. One could imagine a digital dollar that not only shields you from local currency devaluation but also grows at a few percent APY; it would beat many local savings options and potentially drive mass adoption (and do it at a quick rate). However, the typical user’s strategy is basic: acquire USDT or USDC, hold it as a more stable store of value than the local currency, and liquidate when needed. That’s it. The digital dollars sit idle, often earning 0%. During our field trip, a few savvy individuals knew about DeFi lending or staking, but nearly all of them deemed it too complex or too risky.

And it’s hard to blame them - the “DeFi craze” of 2020-2021 did reach Africa’s shores, but mostly among crypto enthusiasts. Those who jumped into high-yield protocols often learned about volatility and various risks the hard way. Stories of scams or sudden losses spread quickly, reinforcing a perception that these schemes are for gamblers or experts.

The result is a yield gap: ordinary users stick to stablecoins for stability and liquidity, while ignoring the yield piece for now. This gap represents a missed opportunity in user experience. Today, attaining yield usually means exiting the simple apps and venturing into DeFi protocols or crypto lending platforms, which few are comfortable doing. One entrepreneur we interviewed in Lagos told us: “if it sounds too good to be true, I stay away - I’d rather lose out on 5% interest than 100% of my money”. This cautious mindset is common, especially after global events like the USDT (Terra) crash and other stablecoin scares underscored that even “safe” assets carry risk. Without easy, built-in incentives to hold long-term, users treat stablecoins as transactional accounts, not full-fledged savings vehicles. To spur adoption, projects will need to introduce user-friendly yield features (perhaps regulated, transparent interest-bearing stablecoins or integrations with low-risk yield sources) that don’t require multiple steps to use. Otherwise, many users will continue cashing out their stablecoins quickly, since holding them confers no advantage beyond the dollar peg.

The stablecoin trilemma of privacy, spendability, and yield is essentially a UX design challenge: how to deliver more of each without sacrificing the others. Solving it won’t be easy, but the reward is immense - a future where anyone, anywhere can use a stablecoin as confidently and effortlessly as they use cash or mobile money. The more stablecoins feel “just like money” - private, usable, and beneficial to hold - the faster adoption will jump from the crypto niche to the mainstream.

Chapter 5:
USX - The first neodollar

The stablecoin trilemma - privacy, spendability, and yield - has remained unsolved because solving it requires infrastructure that didn't exist until recently. Gen-1 stablecoins like USDT and USDC prioritized liquidity and regulatory clarity but left yield on the table and made every transaction public. Gen-2 yield-bearing stablecoins added returns but sacrificed usability, forcing users to unstake, swap, and bridge before they could actually spend their funds. Privacy-focused solutions existed in isolation but offered neither yield nor seamless payment integration.

No stablecoin combined all three. The technological and operational requirements were too complex to layer onto existing infrastructure. Privacy requires a complex zk-layer as its fundament, gasless transactions require subsidized execution that most chains can't support economically, sustainable yield demands access to institutional-grade strategies beyond what typical DeFi protocols can offer, spendability requires payment partnerships and liquidity that niche tokens could struggle to build.

Scroll aimed to change this equation by first perfecting the infrastructure stack over the past 3 years - highest possible security, low-cost execution for gasless transactions, and Cloak for auditable privacy. This foundation makes it possible to build what couldn't be built elsewhere: a stablecoin, USX, that doesn't force users to choose.

Introducing the neodollar category

USX represents a new category of stablecoins - what we call neodollars. The product characteristics fundamentally differ from what came before. A neodollar maintains dollar stability while delivering privacy, yield, and spendability simultaneously. It works like cash (private, instant, universally accepted), earns like an investment account (double-digit ~10-15% sustainable annual returns), and operates like any other savings/bank account (seamless payments, no friction).

USX minting launched in November 2025. Users can now swap USDC for USX one-for-one (+slippage), and KYCed users or institutions can choose to mint it directly. Holders can then stake into sUSX to earn ~10-15% annual returns generated through a combination of offchain strategies and onchain strategies. Every transaction will also be private by default, powered by Scroll's Cloak. And because USX will also be gasless, users will never need to hold ETH or manage gas fees - the aim is for transactions to feel as intuitive as PayPal or Venmo.

Technical architecture: How USX maintains stability, privacy, and yield

USX is fully collateralized, pegged 1:1 to the U.S. dollar. USX’s offchain yield strategies are verified through an external platform which verifies financial data in real-time while preserving privacy. Users can redeem USX for underlying USDC at any time at the 1:1 rate, though redemptions require 14 days processing due to how yield strategies operate - similar to TradFi redemption windows, not a liquidity constraint.

The yield comes from a dual-strategy approach:

- **Offchain market-neutral arbitrage:** Our partnered trading firm runs strategies (including basis trades, spot-futures, and cross-exchange arbitrage) that are uncorrelated to crypto market movements.

- **Onchain delta-neutral strategies:** Blend’s execution layer deploys funds across lending, yield-tranching, and liquidity provision while hedging risk to generate stable, predictable returns.

You can find more information in the documentation (Yield Strategies).

USX’s Reserve Fund

To strengthen capital protection, USX maintains an onchain reserve fund designed to cover potential losses from offchain trading or onchain yield strategies. We're seeding it with $5 million worth of SCR, with a set amount of USX.Capital’s governance token earmarked upon launch.

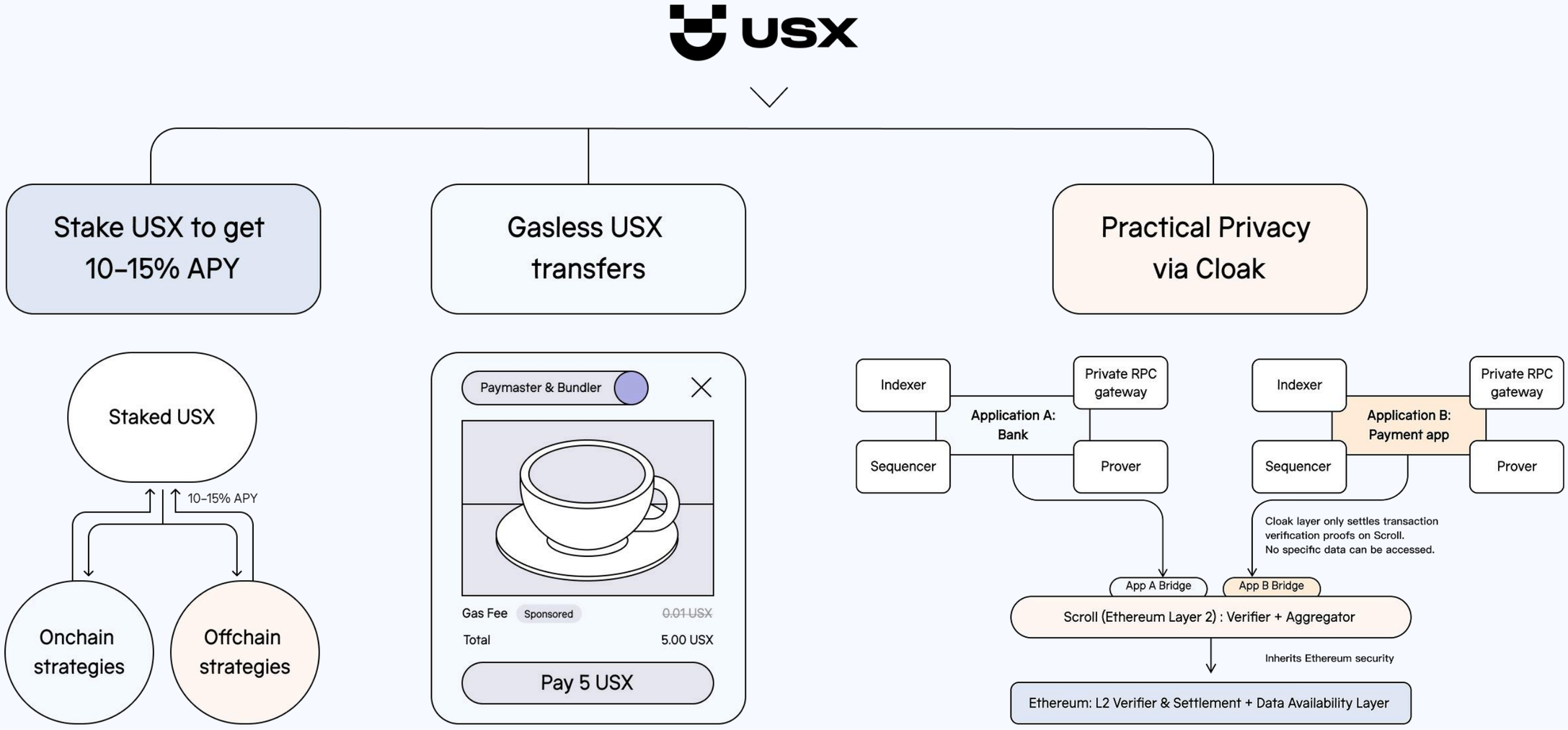
- The protocol allocates 50% of its 10% protocol fee toward building this reserve.
- The fund targets a minimum coverage of 2% of all deployed principal, with no current cap on size.
- It acts as an insurance buffer, protecting the protocol and users from unexpected drawdowns.
- The community will be notified before implementing any changes to the fund.
- The reserve fund contract is published and verifiable onchain here.

You can also find out more about the risks and how we’re mitigating them here.

Privacy

Privacy works through Cloak's architecture. Transactions are shielded from public observation but remain auditable by the protocol and, when required by law, by regulators. We didn’t build for a black-box anonymity - it's the same privacy model banks use, where others can't see your account balance or transaction history, but auditors can request records if needed. For businesses, this means treasury movements stay confidential from competitors. For individuals, it means financial activity isn't permanently published for data brokers to harvest.

If you’re interested to read more about the importance of privacy, I have recently published another report that dives into its history as well as its path forward.



Gasless transactions remove the largest friction point in crypto payments. Users never see gas fees, never need to hold ETH for transactions, never encounter "insufficient funds for gas" errors. The experience feels like any payment app - tap, confirm, done. The protocol handles execution costs in the background.

* All of the features of USX will continue to roll-out across Q4 of 2025 and Q1 of 2026.

Chapter 6:
The opportunity: Building the future with USX

Looking at the history, most of the past revolutions didn’t feel like revolutions at first. Previous centuries teach us that they tend to start quietly, solving mundane problems better than the incumbents, until one day the old way just stops making sense.

Email didn't replace the postal service because technologists declared it superior - it replaced it because sending a letter in three seconds for free was obviously better than paying $0.55 and waiting three days. The internet didn't disrupt retail because of vision documents - it disrupted retail as ordering from your couch beat driving to the mall, and having an answer from Google in 3 seconds was much better than opening an encyclopedia. AI is now the most recent quiet revolution - as it’s starting to quickly reshape how many industries operate.

Stablecoins are also following the same pattern. They aren’t going to replace correspondent banking through ideology, but through very specific corridors - fighting remittances or cross-border payments, higher yield offering than standard saving accounts and faster settlement. The value proposition was concrete enough that hundreds of billions in capital already chose to switch rails despite regulatory uncertainty, interface friction, and the inertia of established systems.

But the first wave of stablecoins solved only part of the problem. They made digital dollars fast and borderless. They didn't make them private. They didn't make them productive. They didn't make them simple enough for your parents to use without a tutorial. The next wave has to solve what the first wave left unfinished.

Why now - and why the window is closing

Three conditions are converging that make 2026-2027 the critical window for next-generation stablecoins:

1. **Regulatory clarity removed the main blocker.** The GENIUS Act, signed into law in July 2025, created the first federal framework for payment stablecoins, mandating full reserve backing, regular audits, and clear licensing requirements. Hong Kong's LEAP framework introduced stablecoin licensing that took effect August 1, 2025. The European Union's MiCA regulations establish similar standards.

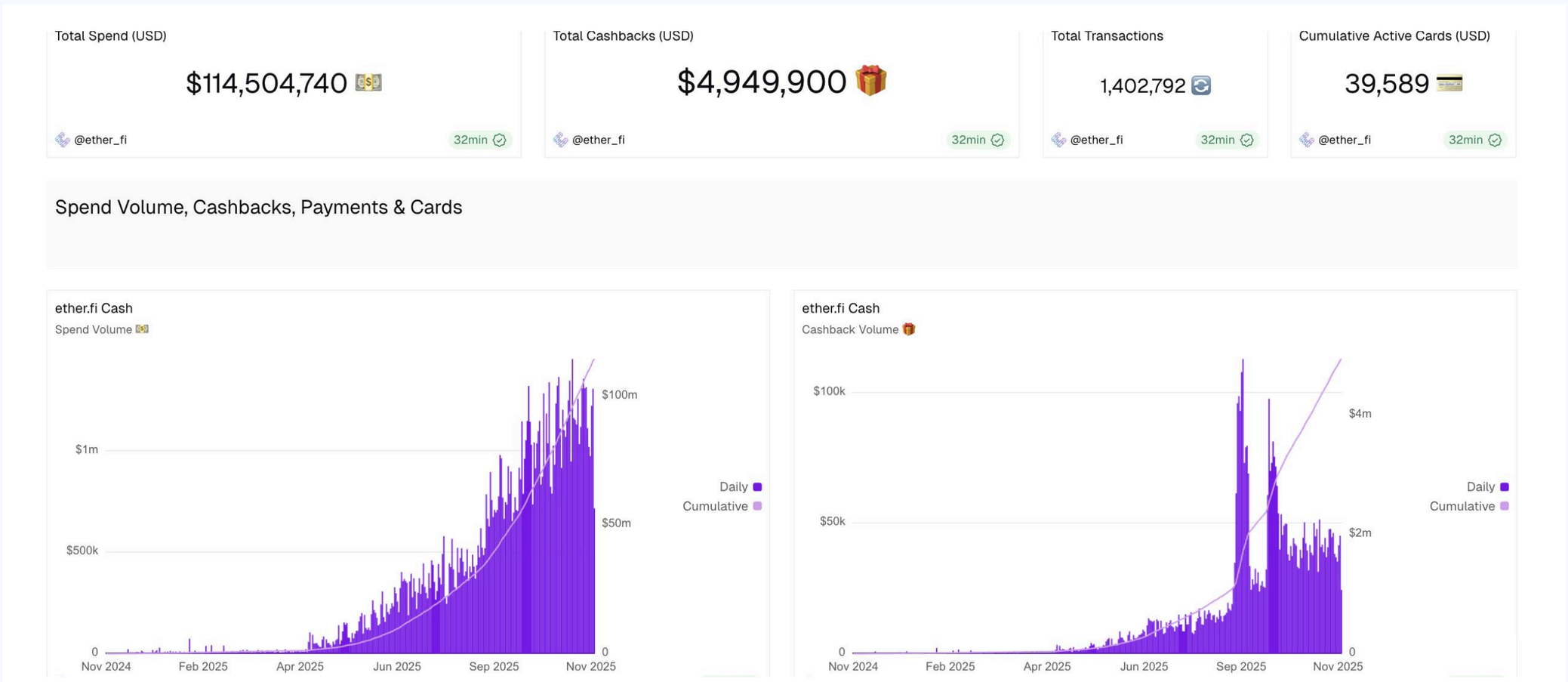
   For years, institutions waited on the sidelines because legal teams couldn't sign off on exposure to assets operating in regulatory gray zones. That barrier is now gone - and the rules are clear. Stablecoins that comply can scale without existential regulatory risk.

   The GENIUS Act also sets a deadline. New U.S. dollar stablecoin issuers must be licensed entities by January 2027. That gives the market roughly 18 months to establish positioning before regulatory gates tighten and compliance costs rise. First movers capture network effects - liquidity, integration partnerships, user bases - that become difficult to displace once switching costs favor incumbents.

2. **Technical infrastructure matured.** Just a few years ago, transacting on a ZK-powered chain that offers robust security was simply expensive. The proving costs were high, with many users choosing to transact on optimistic rollups instead.

   This is no longer the case - for instance, through many protocol upgrades, Scroll is now able to offer transaction fees that regularly come in lower than Base and comparable OP stack chains, despite offering stronger security guarantees and native privacy infrastructure that optimistic rollups can't match.

3. **Market demand is accelerating from both ends.** More and more web2 companies choose to migrate their treasuries onchain, the same way more and more people choose to migrate their financial lives onchain. We have witnessed the rise of many new neobank apps, as well as many new credit/debit card solutions, of which growth has been exponential. One example is the etherf.fi Cash card, which has already processed over 1.4M transactions that totaled over $110M.



User-centric use cases for USX

USX’s design as a zk-native neodollar goes far beyond checking a few technological boxes. It was engineered to unlock new user experiences that weren’t possible with earlier stablecoins.

For individuals: One balance, three problems solved

As this report has outlined in its earlier sections, today's stablecoins force architectural compromises. Earn yield or spend easily, hold dollars or maintain privacy, avoid gas fees or use decentralized infrastructure - pick two.

USX collapses those choices. Users can swap between USDC and USX 1:1, face no gas fees, keep their transactions private, get yield, and spend the stablecoin directly via our payment partners like ether.fi. In this way, people can choose to live their full financial lives onchain, while getting access to a much higher yield than what standard banks offer.

Institutional use cases for USX

USX’s feature set is equally compelling for institutions and enterprises, who have been cautiously waiting for a stablecoin that meets their stringent requirements.

Institutions are increasingly interested in DeFi, but they need transaction privacy and predictable execution. USX provides settlement confidentiality that institutional capital requires. Large trades, protocol migrations, portfolio rebalancing - all shielded from public observation while remaining auditable for compliance.

USX eliminates architectural trade-offs. Corporate reserves held in sUSX earn 10-15% backed by institutional-grade risk management. Payments to vendors, contractors, employees flow directly from treasury without intermediate conversions. Transaction details stay confidential - competitors analyzing onchain activity can't infer burn rates, hiring patterns, supplier relationships through wallet surveillance.

Public companies can hold operational cash onchain, demonstrate to investors that capital generates returns rather than sitting idle, maintain transaction privacy for competitive advantage, and retain instant liquidity for working capital needs. That combination couldn't exist before because no stablecoin architecture supported all four requirements simultaneously.

The opportunity extends beyond replacing existing treasury operations wholesale. The real wedge is upgrading the portion of corporate cash currently earning nothing while blockchain infrastructure offers superior returns with comparable risk profiles and better operational flexibility.

What gets built in the next 18 months shapes the next decade

We’re entering the final design phase of what money on the internet will become. Not just how it moves - but how it protects, rewards, and empowers the people using it. In this moment, the biggest opportunity isn’t scale. It’s reinvention. A new generation of stablecoins is arriving not to iterate on what worked, but to challenge what didn’t. Privacy isn’t optional, spendability isn’t a UX feature, and yield isn’t a cherry on top. These are the pillars of programmable, usable money - and the reason USX exists.

If you’re building apps, products, or treasury systems for this new wave of stablecoins, now’s the moment to move. Minting for USX goes live this November, with limited spots open for early integrations. Join the teams deploying capital, unlocking new markets, and delivering true financial UX to their users.

Moments like this don’t come often.

The rails are in place, the technology has proven to work, and the use cases are waiting to be built on top of it.

What’s left is for builders, founders, and forward thinkers to step in.

The opportunity is now in your hands.

Get in touch

We designed USX to be the new chapter of finance, to reset what users and builders can expect from digital dollars.
If you’re ready to help define its story, we’d love to build with you.

Learn more about USX

Website: https://www.usx.capital/

Documentation: https://scroll-zkp.gitbook.io/usx

Connect with our BD team

@Filip_bd

or email at contact@usx.capital

Connect with me on LinkedIn

www.linkedin.com/in/sandy-peng-