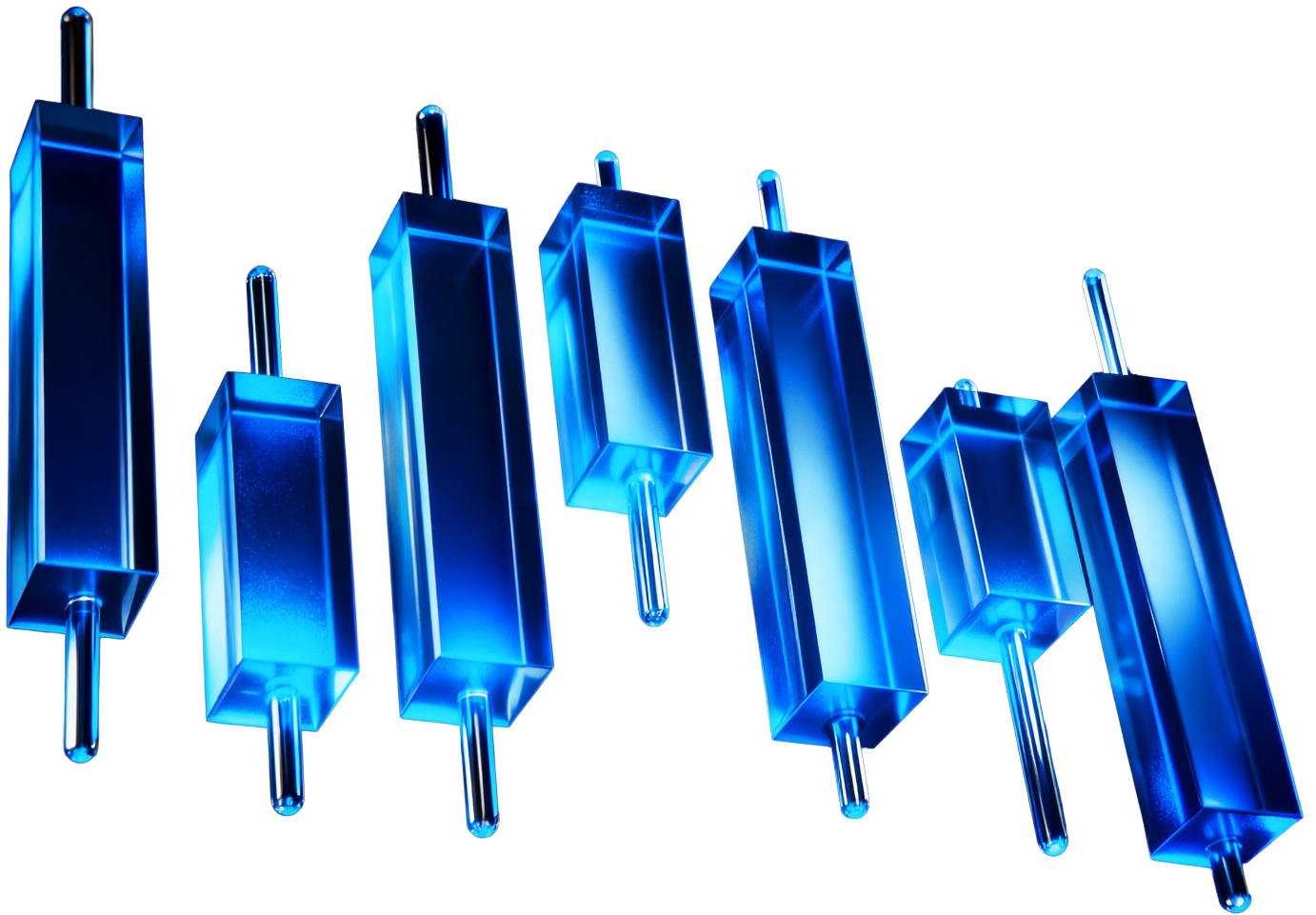




A Market Structure Framework for Resilient Digital Asset Markets

Why custody, credit, trading, and settlement should never share a single point of failure

Contents

3	—	Abstract
3	—	In Digital Assets, Custody Is Market Structure
4	—	01 The Architecture of Resilience in U.S. Capital Markets
6	—	02 How Centralized Exchanges Rebundle Market Functions
7	—	03 Bearer-Asset Custody and the Limits of Reserve Transparency
8	—	04 The Empirical Failure Record
10	—	05 Exchange-as-Lender: Credit, Leverage, and Contagion
10	—	06 Concentration Risk and the Measurement Problem
11	—	07 The Isolation Framework
13	—	08 Policy Pathways and Institutional Adoption
14	—	Conclusion
15	—	Sources

Abstract

When a centralized crypto platform fails, the failure usually lands on customers. The reason is structural. U.S. securities markets keep trading, brokerage, custody, clearing, settlement, and credit in separate hands, while centralized crypto platforms tend to fold all of those functions into a single company. Because cryptoassets are bearer-like instruments whose control follows control of a private key, that bundling lets a custody, credit, governance, or operational failure in one place become a frozen account or a permanent loss for customers. A proposed remedy is functional isolation: trading, custody, credit, clearing, settlement, and affiliated market-making held apart, so that no single failure can take down the rest.

In Digital Assets, Custody Is Market Structure

In traditional U.S. securities markets, the work of running a market is spread across many institutions. Exchanges match orders. Broker-dealers intermediate customer orders under capital and customer-protection rules. Clearing agencies compare, net, and guarantee obligations. The Depository Trust Company (DTC) moves securities and supports book-entry settlement. Securities Investor Protection Corporation (SIPC) steps in when a member broker-dealer fails and customer property is missing. The system is imperfect, but it is deliberately layered: a trading outage at an exchange does not touch a customer's ownership of their securities, and a broker-dealer liquidation runs through a different legal channel than an exchange technology failure.

A centralized crypto exchange usually works the other way. A single platform may onboard the customer, control the wallets, keep the internal ledger, match orders, lend on margin, run derivatives, liquidate accounts, hold collateral, offer staking and yield, list its own affiliated tokens, route flow to affiliated market makers, and settle everything on its own books before anything moves on-chain. This is convenient. It removes friction, supports trading around the clock, sidesteps slow fiat rails, enables unified margin, and lets users trade without managing keys. It is also fragile in a specific and dangerous way.

The fragility comes from what a digital asset is. A share of stock is not transferred by whoever happens to know a password; ownership lives inside a legal and intermediated system. A cryptoasset is closer to a bearer instrument. Whoever controls the private key or signing authority can move it, and an on-chain transfer can settle with finality long before a court can weigh in. A platform that controls keys can move customer assets. So can a hacker who compromises signing authority, or an insider who controls the ledger and the withdrawal system. In each case the customer-asset problem is created before anyone has determined who legally owned what.

That is why custody, in digital assets, is not an operational detail sitting beneath market structure. It is a fundamental piece of the overall market structure. The record bears this out: across more than a decade of failures, the recurring pattern is a custody, credit, operational, or governance breakdown becoming a customer-asset event precisely because all of those functions lived inside one company.

The argument proceeds in eight sections: the layered architecture of U.S. capital markets; how centralized crypto exchanges rebundle those functions; the bearer-asset custody problem and the limits of proof-of-reserves; the empirical failure record; exchange-as-lender contagion; concentration risk and what public data can and cannot measure; a proposed isolation framework; and policy and institutional adoption pathways.

The Architecture of Resilience in U.S. Capital Markets

U.S. capital markets are resilient because they are layered, and that layering was not designed in the abstract. It was built up over decades, each rule a response to a specific failure.

The statutory core is the Securities Exchange Act of 1934, which set the framework for exchanges, broker-dealers, clearing agencies, transfer agents, and market oversight. Exchanges register or qualify for an exemption. Broker-dealers register and comply with financial responsibility rules. Clearing agencies register and must support prompt, accurate clearance and settlement. Self-regulatory organizations operate under SEC supervision. The effect is to separate market access, execution, custody, clearing, settlement, capital, surveillance, and customer-asset protection into distinct categories with distinct rules.

Two of those rules do most of the work in protecting customer assets. The Customer Protection Rule (Rule 15c3-3) requires broker-dealers to keep possession or control of fully paid and excess margin securities and to maintain a reserve for customer benefit. The Net Capital Rule (Rule 15c3-1) requires them to hold enough liquid capital that customer property never becomes the firm's working capital. SIPA adds a backstop: under SIPA, a failed broker-dealer with missing customer property enters a special, trustee-supervised liquidation built to return customer securities and cash. Settlement and custody sit in another layer entirely, managed by DTC subsidiaries like NSCC and DTC, whose depository and net-settlement services are wholly separate from the matching of trades on an exchange. Clearing agencies are themselves regulated under Rule 17Ad-22, and Regulation SCI governs the resilience of the technology systems running beneath all of it.

This separation matters because it does several things at once. It reduces single points of failure, limits conflicts of interest, gives customer-asset protection that does not depend on any one venue's solvency, clarifies who supervises what, and supports orderly recovery. An exchange outage, a market-maker failure, a broker-dealer capital shortfall, and a clearing deposit shock are four different problems with four different responses.

History shows the pattern holding even under severe stress. The 1987 crash was a market-wide event with trading, margin, credit, and liquidity dimensions, not an exchange-custody failure. Lehman Brothers showed that a broker-dealer and investment bank can collapse catastrophically, yet the broker-dealer's customer securities moved through a SIPA liquidation rather than vanishing with the firm. Knight Capital's 2012 software failure nearly destroyed the firm through erroneous orders but never converted into custody loss. Nasdaq's botched Facebook IPO, the 2015 NYSE halt of all symbols for three hours and thirty-eight minutes, and the 2023 NYSE opening-auction disruption that affected more than 2,800 securities all impaired trading without becoming customer-asset losses. In January 2021, Robinhood restricted buying in GameStop and other names under clearinghouse deposit pressure; customers lost access to certain trades, but the mechanism was broker-clearing liquidity, not exchange custody. Archegos, that same year, was a prime-brokerage leverage failure that cost banks billions through total return swaps, again separate from exchange custody.

The one true counterexample is MF Global, where customer funds were in fact impaired, and it is worth dwelling on because it proves the rule rather than breaking it. The CFTC has described customer-fund segregation as fundamental, and the Commodity Exchange Act prohibits commingling customer and proprietary funds. MF Global violated those rules and supervision failed to catch it in time. What followed was a trustee process, which ultimately achieved a 100% recovery of customer property, and a renewed enforcement focus on segregation controls. The lesson was not that separation is irrelevant. It was that segregation rules are exactly what stand between a firm's collapse and its customers' money and that the rules must be actively enforced to do that work.

The through-line is simple. Failures happen inside the layered system too, but because execution, custody, clearing, settlement, credit, and capital are not controlled by one entity, a shock in one layer was less likely to cascade into losses across all of them. Classification here is not bureaucratic tidiness; it determines how recovery, supervision, liability, and customer-asset treatment actually play out.

Event	Failure type	Customer-asset impact	Recovery and response	Role-separation lesson
1987 Crash	Market crash, liquidity stress, feedback trading	Market losses, not custody loss	Market stabilization; circuit breakers introduced	Severe market failure without exchange-custody collapse
2008 Lehman Brothers	Insolvency, liquidity run, counterparty failure	Broker-dealer customer-property process, not custody loss	SIPA liquidation for the broker-dealer; parent bankruptcy	Legal-entity and customer-property channels held
2011 MF Global	Customer-fund segregation failure	Yes, funds impaired	Trustee process; restitution; segregation enforcement	Counterexample: customer-asset rules need supervision
2012 Knight Capital	Technology and market-access failure	No public custody loss	Capital rescue and acquisition; enforcement	Operational trading failure did not become custody loss
2012 Nasdaq Facebook IPO	Exchange systems and IPO process failure	No public custody loss	Claims process; regulatory settlement	Venue and process failure stayed separate from custody
2015 NYSE all-symbol halt	Systems outage	No public custody loss	Trading shifted to other venues; reopened same day	Venue outage did not control customer assets
2021 Robinhood / GameStop	Clearing-deposit and liquidity stress	Trading restrictions, not custody loss	Deposit adjustments; capital raise; hearings	Broker-clearing liquidity limited access, not custody
2021 Archegos	Leverage, swaps, counterparty risk	Bank losses, not exchange-custody loss	Bank write-downs; prosecutions; risk reviews	Prime-brokerage leverage differs from venue operation
2023 NYSE opening-auction disruption	Opening-auction systems failure	No public custody loss	Busted trades; SEC settlement	Market-operation failure stayed in the trading layer

Table 1. Traditional-finance failures and how role separation contained them.

How Centralized Exchanges Rebundle Market Functions

A large bundled crypto exchange is not a digital NYSE. It is closer to a single institution that is at once an exchange, a retail broker, a custodian, a clearing utility, a margin lender, an internal settlement system, a staking agent, a token-listing authority, an affiliated market maker, a proprietary trading desk, and a collateral issuer, all inside one balance sheet and one governance perimeter. International bodies have named the pattern. The Financial Stability Board describes multifunction crypto-asset intermediaries that combine trading, brokerage, dealing, market-making, custody, clearing, settlement, lending, borrowing, and issuance, while IOSCO's recommendations target the conflicts, custody, and client-asset risks that follow.

At minimum, the typical centralized exchange bundles four functions: it matches trades, it controls customer assets through omnibus wallets, it maintains the internal customer ledger, and it settles customer transfers on its own books before anything moves on-chain. Most then add more, including margin lending, perpetual futures, staking, Earn products, token issuance, and affiliated trading. The SEC's complaints against Coinbase and Binance turned on these structural dynamics, alleging that the platforms ran combinations of exchange, broker, clearing, and other functions without registration. Those were allegations rather than final rulings, and later policy shifts changed the enforcement posture, but the structural concern they identified is independent of any single case.

Bundling did not arise from carelessness; it solved real problems. Self-custody is hard. Fiat settlement is slow. Crypto prime brokerage was immature. Markets that trade around the clock need collateral to move continuously. Retail users want one account and instant transfers, derivatives traders want unified cross-margin, and exchanges want to own both the customer relationship and the economics of custody, lending, and listings. The honest case for bundling is efficiency: integrated custody and trading cut settlement friction, make small trades practical, lower onboarding barriers, allow internal netting, and relieve users of managing keys, gas, congestion, and bridge risk.

The problem is that efficiency cannot be allowed to override resilience, and in a bundled model the two trade off directly. Commingling can obscure whether customer assets are held in trust, lent out, rehypothecated, pledged, or merely recorded as a platform liability. Rehypothecation quietly turns custody into credit. An internal ledger can drift away from the assets actually in the wallets. Affiliate exposure moves risk from a trading arm onto the venue. Exchange-issued tokens can become circular collateral. Proof-of-reserves can show assets while saying nothing about the full set of liabilities, so that a wave of customer withdrawals becomes the first real test of solvency. And bankruptcy remoteness, a critical protection when a platform fails, is often uncertain.

The comparison with equities makes this vivid. In equities, the exchange does not hold the customer's fully paid shares, the broker-dealer is bound by possession-or-control and reserve rules, clearing and settlement run through regulated infrastructure, and if the broker fails a specialized liquidation returns customer property. In a bundled crypto exchange, one entity is the venue, broker, custodian, settlement ledger, and lender at the same time. DeFi does not dissolve this problem so much as relocate it: moving to self-custodied interaction with smart contracts trades intermediary risk for smart-contract bugs, oracle manipulation, bridge failures, governance attacks, and liquidation cascades. It is a different intermediation, not the absence of one.

¹ IOSCO, Tokenization of Financial Assets Final Report (FR/17/2025), Codezeros, "From Paper to Protocol: How Trust Companies Became the Backbone of RWA Tokenization," October 2025.

Bearer-Asset Custody and the Limits of Reserve Transparency

Digital asset custody differs from securities custody because technical control can be practical control.

A security held in the U.S. system is a chain of book-entry entitlements running through a broker-dealer, a clearing participant, and DTC. That chain carries real risks, including intermediated title, omnibus accounts, securities lending, and failed settlements. But a share of stock is not transferred simply by possessing cryptographic data. A cryptoasset is. Control of the keys or signing authority is the power to move the asset, and once a transfer settles on-chain it is effectively irreversible, often before anyone can intervene. Wallet architecture, signer permissions, quorum rules, and withdrawal controls are therefore not back-office plumbing. They are part of market design.

This opens a gap between legal custody and technical key control, and a resilient market has to close both sides of it. Legal custody asks who owes duties to the customer, what the customer actually owns, whether assets are segregated or held only as a platform liability, and what happens in bankruptcy. Technical key control asks a different set of questions: who can move the asset, how many approvals are required, whether signing devices are online, whether withdrawals are rate-limited, and whether insiders can override the controls under stress. The machinery behind those questions includes hot, warm, and cold storage, multisignature and MPC schemes, hardware security modules, allowlists, withdrawal delays, approval workflows, and key-compromise procedures, and each control changes who can move assets and how fast a compromise turns into a loss.

Cold storage is the headline metric, and the disclosed benchmarks are real. Coinbase has described a target of holding no more than 2% of assets under custody in hot wallets, while OKX, Bitstamp, and Bitget have cited roughly 95% or more in cold storage. Those numbers are useful, but the 2025 Bybit incident showed their limits. That was not a simple hot-wallet theft. It was a compromise of the cold-wallet signing workflow itself, which means the label cold storage did not, on its own, describe the actual risk.

Proof-of-reserves runs into a similar ceiling. A reserve attestation can show that a platform controls wallets holding certain assets, and a Merkle-tree liability proof can let a customer confirm their balance was included in a disclosed liability set. What neither can do is prove solvency. They can miss off-balance-sheet liabilities, affiliate claims, pledged or rehypothecated assets, undisclosed borrowings, derivatives exposure, and senior claims. A platform can prove it controls wallets and still fail to prove customers own what is in them; it can show a flattering snapshot taken at the right moment; it can leave affiliated exposure out of the picture entirely. What a customer critically needs to know is not only that assets exist, but that they are not pledged, lent, subordinated, or subject to competing claims.

Bankruptcy is where the distinction becomes highly consequential. A customer who believed their assets were in custody may find that the terms of service, commingling, or a title-transfer clause converted the relationship into an unsecured claim. Celsius is a clear example: the bankruptcy court held that Earn assets were property of the debtor estates under the terms of use. Custody, properly understood, therefore has three layers that must all hold: technical control of the keys, enforceable legal entitlement, and bankruptcy-remote treatment when the platform is gone. A market that secures one or two of the three is not secure.

The Empirical Failure Record

More than a decade of failures tells one structural story, even though the cases themselves are very different from one another. The mistake to avoid is summing every theft, freeze, and delayed claim into a single headline loss number, because the cases are not interchangeable. Mt. Gox was an exchange-custody collapse. Coincheck was a hot-wallet breach followed by corporate reimbursement. Bitfinex was a hack resolved through a recovery token. QuadrigaCX was a collapse the Ontario Securities Commission attributed to fraud by its CEO and to missing reserves. Celsius, Voyager, BlockFi, Genesis, and Gemini Earn were credit and yield-product failures with very different customer outcomes. Three Arrows Capital was not a retail exchange at all but a contagion node. Bybit was a large custody-signing compromise the exchange survived. What unites them is the mechanism, not the magnitude: in these instances, a failure in one bundled function becomes a customer-asset event.

The numbers, kept in their proper categories, make the point. Mt. Gox is the long-duration custody failure: roughly 850,000 BTC were initially reported missing and about 200,000 were later recovered, a gross unit-recovery signal of 23.5% before any legal-claim mechanics, with repayments beginning in 2024 and the deadline since extended to October 31, 2026, more than a decade after the collapse. Coincheck shows direct key-control failure resolved by the corporate balance sheet: 58 billion yen, about 532.6 million dollars, in NEM was taken in a hot-wallet breach, and the company reimbursed roughly 46.3 billion yen, a 79.8% fiat-value signal that preserved fiat value through the chosen method rather than restoring the asset itself.

Bitfinex is a hybrid resolution. The Department of Justice later put the 2016 hack at roughly 120,000 bitcoin; Bitfinex reports 119,755 BTC stolen and that affected customers received BFX tokens equal to their dollar losses, later redeemed at par or converted to equity. That was a corporate recovery mechanism, not evidence that the custody failure was harmless. QuadrigaCX is a case of false balances and missing reserves: the Ontario Securities Commission concluded that the platform's downfall was caused by fraud committed by its CEO, with about C\$215 million owed to clients.

The credit and yield cases round out the record. Celsius froze withdrawals, filed for Chapter 11, and saw its Earn assets ruled property of the estate. Voyager, caught by its exposure to Three Arrows Capital, made an initial distribution of roughly 35.7% of claims in 2023, with a second distribution in 2024–2025 pushing cumulative recovery past 70% for many creditors, the final figure still dependent on 3AC litigation. Genesis and Gemini Earn are the important counterexample: Gemini announced that Earn users recovered \$2.18 billion in digital assets in kind, a full recovery, but only after an extended freeze, which supports the structural point that a credit-intermediation chain cost customers access and control. Three Arrows transmitted its leverage through centralized lending channels. And Bybit, hit in February 2025 by a roughly \$1.5 billion theft the FBI attributed to North Korean actors, reported customer holdings safe, an example of a custody-control failure that did not become a customer insolvency.

Event	Failure and scale	Recovery treatment	Customer-asset and bundled-function treatment	Thesis relevance
2014 Mt. Gox	Exchange-custody collapse; ~850,000 BTC reported missing	23.5% gross unit signal from 200,000 BTC found; repayments from 2024; deadline to Oct. 31, 2026	Weak custody controls; exchange, custody, and internal ledger; long claim process	Custody failure became customer-asset impairment
2016 Bitfinex	Hack and custody compromise; 119,755-120,000 BTC stolen	BFX tokens redeemed at par or converted to equity; later law-enforcement recovery	Omnibus exchange custody; platform-level recovery mechanism	Theft required a recovery mechanism inside the platform

continued on next page →

Event	Failure and scale	Recovery treatment	Customer-asset and bundled-function treatment	Thesis relevance
2018 Coincheck	Hot-wallet NEM theft; 58B yen, about \$532.6M	About 46B yen reimbursed; 79.3% fiat signal	Exposed hot-wallet infrastructure; fiat repayment basis	Direct key-control failure became a reimbursement event
2019 QuadrigaCX	OSC-attributed fraud; false balances; missing reserves	C\$46M recovered by the trustee; C\$39.7M (13%) interim distribution against C\$303.2M in filed bankruptcy claims, a later, larger figure than the C\$215M the OSC found was owed at collapse	Not effectively segregated; balances became claims	False ledger and custody converted balances into claims
2022 Three Arrows Capital	Leveraged fund insolvency; billions in claims and lender exposure	Recovery uncertain and proceeding-dependent	Not retail custody; fund leverage and lender exposure	Fund leverage transmitted losses through credit channels
2022 Voyager	Credit failure; balances frozen; large 3AC exposure	Initial ~35.7% distribution (2023); cumulative recovery above 70% after 2024–2025 distributions; final figure still claim-dependent	Entitlement via bankruptcy claims; brokerage, yield, lending	Lending exposure froze customer platform balances
2022 Celsius	Yield-product credit failure; withdrawals frozen	Crypto, fiat, and equity distributions; varies by account	Earn ruled estate property; custody-like accounts plus lending	Custody-like balances became estate and credit claims
2022 BlockFi	Credit failure; claims frozen	Class-dependent; settlement up to \$874M with FTX Estate.	Claim treatment by product; lending and custody-like accounts	Counterparty exposure turned balances into claims
2022–2024 Genesis / Gemini Earn	Lending freeze after Genesis distress; Earn assets frozen	Gemini announced 100% in-kind recovery after settlements	Earn structure, not simple segregated custody	High recovery still followed an extended credit-chain freeze
2025 Bybit	Wallet signing-workflow compromise; ~\$1.5B stolen	Final recovery not public; exchange reported holdings safe	Customer-solvency impact not publicly final; exchange and custody	Cold-wallet workflow failed without platform collapse

Table 2. Major crypto exchange, custody, and credit failures, kept in separate recovery categories.

The strongest objection to all of this is that the word loss overstates the damage when recoveries are high, and in several cases that is fair. Gemini Earn users recovered in kind, Bitfinex customers were made whole through BFX tokens, and Coincheck reimbursed in fiat. But none of that dissolves the structural problem. A delayed recovery is not uninterrupted custody. A corporate reimbursement is not a resilient architecture. Even a high bankruptcy recovery still means that market access, legal entitlement, liquidity, and asset control were simultaneously disrupted, which is exactly the outcome separation is meant to prevent.

05

Exchange-as-Lender: Credit, Leverage, and Contagion

When one entity is exchange, lender, and custodian at once, market volatility and the platform's own solvency stop being separate variables. The exchange-as-lender model takes many forms, including margin lending, perpetual futures, Earn and lending products, staking, proprietary trading affiliates, exchange-issued tokens used as collateral, and outright rehypothecation of customer assets. Each one converts custody into leverage.

The failure sequence is familiar. Prices fall, collateral drops, leveraged users are liquidated, affiliated lenders absorb the losses, customers rush to withdraw, confidence breaks, and liquidity disappears. The bundling is what links each step to the next.

Celsius shows this inside a single entity. Its Earn product paid yield on deposited crypto, so customer assets were not in segregated custody but were lent out and staked to fund the returns, with custody, credit, and yield on one balance sheet. When those positions soured and customers moved to withdraw, Celsius could not meet redemptions; it froze withdrawals in June 2022 and filed for Chapter 11. The court later ruled Earn balances were property of the estate, leaving customers who thought their assets were in safekeeping as unsecured creditors.

Three Arrows Capital shows the same flaw spreading across firms. The leveraged fund defaulted on its loans in the 2022 downturn, and the losses passed straight to the platforms that had lent to it. Voyager, exposed for hundreds of millions, froze customer accounts and entered bankruptcy. An ordinary fund blowup became frozen retail accounts because the lending and the deposits sat in the same institutions. Bundling didn't cause the bad bet; it determined how far it could travel.

06

Concentration Risk and the Measurement Problem

Digital asset markets carry two kinds of concentration risk, and public data measures one far better than the other. Flow concentration, meaning how trading volume clusters in a few venues, is observable. Custody concentration, meaning how much customer property actually sits where, is not.

On the flow side, CoinGecko's 2025 top-10 centralized-exchange spot dataset shows Binance at 39.2%, Bybit at 8.1%, and MEXC at 7.8%, a combined top-three share of 55.1% on \$18.7 trillion of volume. The denominator matters: that 55.1% is a share within the top-10 dataset, not a claim about all global CEX volume. Regulators see the same shape from a different angle, with ESMA's analysis finding the top 10 exchanges handling roughly 90% of trading and Binance around half in the period studied. Sources and timing differ, but the conclusion is stable. Flow is concentrated.

Custody concentration is the harder and more important number, and it largely cannot be measured from outside. Exchange-reported reserves are not all customer assets. Wallet labels are incomplete, some exchange wallets are unidentified, and labeled wallets can mix operating balances, market-maker assets, corporate treasury, and customer funds. Hot, warm, and cold classifications are not standardized, proof-of-reserves methods differ, and liability proofs are not universal. Above all, a wallet balance inherently cannot reveal whether the assets in it are pledged, lent, encumbered, or subject to senior claims. Public data can show where volume flows and roughly how large reserves appear; it cannot show where customer custody is concentrated, how it is segregated, or whether it is solvent.

Table 3 compares failure domains across three structures, from today's bundled exchange to full role separation; it is an illustration of where risk sits, not a solvency estimate. The structural point is simple: custody can be moved outside the trading venue without taking trading access with it

Dimension	Current bundled-exchange model	Partially separated model	Fully role-separated model
Custody	Exchange-controlled wallets and internal ledgers	About 46B yen reimbursed; 79.3% fiat signal	Exposed hot-wallet infrastructure; fiat repayment basis
Credit	Exchange, affiliate, internal margin desk, or platform lender	Mix of exchange margin, prime brokers, and lenders	Separately capitalized lenders, prime brokers, or clearing members
Trading venue role	Matching, custody, onboarding, liquidation, internal ledger, product provider	Venue matches trades and still controls some collateral	Venue matches orders; does not custody customer assets
Settlement	Internal book transfers plus on-chain withdrawals	Hybrid off-exchange settlement; prefunded trading; custodial networks	Independent clearing and settlement with transparent collateral rules
Main risk concentration	Venue becomes custody, credit, settlement, and liquidity hub	Retail and derivatives stay concentrated; institutional spot risk reduced	Custody shifts to custodians; credit shifts to lenders and clearing entities
New risk introduced	Single failure domain; commingling; withdrawal-run risk	Custodian concentration; latency; fragmented liquidity	Custodian systemic concentration; operational coordination; higher cost

Table 3. Concentration and risk-transfer scenarios. The model compares failure domains; it is not a solvency estimate.

The honest counterargument is that independent custody simply relocates concentration: if a few custodians end up holding most digital assets, a custodian failure, key-management breakdown, cyber incident, or legal dispute could itself become systemic. That is true. Separation redistributes risk rather than erasing it. The answer is custodian resilience built to a high standard, meaning capital, audited controls, key-management standards, recovery planning, legal segregation, bankruptcy remoteness, insurance disclosure, sub-custodian controls, concentration reporting, and stress-tested transfer procedures. Concentrated risk that is capitalized, supervised, and resolvable is a far better position than concentrated risk hidden inside a trading venue's balance sheet.

07 The Isolation Framework

The objective of the framework is narrow and specific: to keep trading, custody, credit, clearing, settlement, and affiliated market-making from failing together. Everything else follows from that single principle of functional isolation.

In practice it means a venue that matches orders without holding customer assets; a supervised broker or intermediary handling customer access under best-execution and routing rules; an independent, qualified custodian with both legal segregation and audited key controls; clearing and settlement run by parties separate from the venue, with real finality and reconciliation; credit extended by separately capitalized lenders or prime brokers under explicit rehypothecation limits; derivatives collateral and staking assets segregated rather than pooled; affiliated market makers walled off with information barriers and related-party disclosure; proof-of-assets paired with proof-of-liabilities and audited controls; and predefined customer-asset transfer playbooks for distress, rather than ad hoc withdrawal halts.

Table 4 maps each function from its current bundled form to its isolated structure and the control that makes the isolation real.

Dimension	Current bundled model	Proposed isolated structure	Required control
Trading venue	Exchange matches orders and holds assets	Non-custodial venue, or venue with a limited operating buffer	Rulebook, surveillance, outage procedures
Customer access	Exchange acts as broker and account provider	Supervised digital-asset broker or agency intermediary	Best execution, disclosure, customer-asset routing
Custody	Exchange-controlled omnibus wallets	Independent custodian with legal segregation and technical key controls	Audited key governance, sub-custodian oversight, insurance disclosure
Clearing	Internal netting and liquidation engine	Independent clearing or settlement-risk manager	Margin methodology, default rules, stress tests
Settlement	Internal ledger until withdrawal	On-chain or custodial settlement with enforceable finality	Finality rules, reconciliation, fail procedures
Credit	Exchange margin desk or affiliate lender	Separately capitalized lender or crypto prime broker	Capital, collateral rules, rehypothecation limits
Derivatives collateral	Exchange holds collateral and liquidates	Segregated collateral with independent margin governance	Customer-collateral segregation, liquidation transparency
Staking	Exchange pools customer assets and offers yield	Segregated staking agent with slashing and lockup disclosure	Validator controls, slashing disclosure, exit procedures
Lending / Earn	Platform accepts assets and offers yield	Separately disclosed credit product, not custody	Risk disclosure, capital, title-transfer clarity
Market making	Affiliate trades on the venue	Independently capitalized maker with conflict controls	Information barriers, surveillance, related-party disclosure
Proof and audit	Reserve snapshots	Proof-of-assets plus proof-of-liabilities plus audited controls	Independent attestation, liability completeness, audit scope
Resolution	Ad hoc withdrawal halt and bankruptcy	Predefined customer-asset transfer and distress protocols	Living will, transfer playbooks, legal opinions

Table 4. Proposed role-separated digital asset market structure. The required controls shown are illustrative, not exhaustive.

Some traditional-finance principles carry over cleanly: segregation, capital requirements, custody independence, conflict controls, clearing discipline, market surveillance, and recovery planning. Others have to be adapted to the technology. Private-key control has no equity-market equivalent. On-chain finality compresses the time between error and irreversible loss. Wallet governance is itself an asset-control system. Stablecoins may be settlement assets, credit instruments, or payment liabilities depending on how they are built. Markets run around the clock, offshore venues can reach U.S. users indirectly, self-custody remains a genuine alternative, and DeFi interfaces do not map neatly onto the broker-exchange-custodian categories.

That last point invites the strongest crypto-native objection: that digital assets should not copy traditional finance directly, because blockchains allow direct settlement, self-custody, programmable escrow, and transparent collateral. Where users genuinely self-custody and interact with protocols directly, that argument holds. It fails the moment customers deposit assets into a centralized platform that controls the keys, the ledger, liquidation, credit, and withdrawals, which remains common even among platforms that market themselves as decentralized. No intermediary should be able to claim the self-custody virtues of DeFi while keeping the asset control of a centralized exchange.

Offshore competition is a real constraint, not a refutation. If U.S. rules become too slow or costly, activity can move offshore, but that changes implementation rather than the principle. Institutional capital, regulated stablecoin issuance, bank and ETF custody, and U.S.-facing market access can each make functional isolation a condition of participation.

The test of the framework is what it is designed to mitigate. A venue can fail without customers losing their assets. A lender can fail without freezing spot custody. A custodian can fail without corrupting price discovery. A market maker can fail without draining customer collateral. And settlement stress can be handled by transparent rules instead of hidden platform discretion.

08 Policy Pathways and Institutional Adoption

Functional isolation can arrive through regulation, through market pressure, or through institutional adoption, and it does not depend on any single statute.

In the United States, the authority is fragmented. The SEC oversees securities markets, broker-dealers, exchanges, clearing agencies, advisers, and funds; the CFTC oversees derivatives markets and their intermediaries along with commodity anti-fraud and anti-manipulation enforcement; banking regulators supervise banks and some trust activities; state regimes such as the NYDFS virtual-currency and trust-company frameworks regulate certain custodians; and bankruptcy courts decide what is estate property when a platform fails. The SEC and CFTC have used enforcement and interpretation while Congress has weighed market-structure legislation. Stablecoin legislation can sharpen reserve, redemption, and issuer standards, but it does not by itself separate exchange custody, margin, internal ledgers, and affiliated market-making. Stablecoin resilience is necessary for settlement liquidity; it is not sufficient for market-structure resilience.

The more durable organizing idea is that policy should follow function. A platform that holds customer assets should meet custody standards. A platform that lends customer assets should disclose credit risk and capital treatment. A venue that matches orders should have market rules and surveillance. A clearing function should have margin, default, and governance rules. A stablecoin issuer should meet reserve and redemption standards. A market-making affiliate should face conflict-of-interest controls. International policy already points this way: the FSB calls for comprehensive regulation of cryptoasset activities and global stablecoin arrangements, IOSCO's recommendations center on custody, conflicts, client-asset protection, and market integrity, the EU's MiCA framework governs issuers and service providers, and the UK FCA has proposed rules for stablecoin issuance and cryptoasset safeguarding.

Separation has real costs. It can raise expenses, reduce capital efficiency, fragment liquidity, add latency, require prefunding or credit lines, create new custodian concentration, push some retail activity offshore, and sit awkwardly with certain DeFi structures. Those tradeoffs are genuine. The question is only whether they cost less than the alternative, which is letting custody, credit, trading, and settlement keep failing as one.

Institutions may force the issue before regulators do. Asset managers, ETFs, pension fiduciaries, endowments, insurers, banks, advisers, and market makers need clear custody, audit, legal entitlement, and operational controls before they allocate at scale, and spot crypto ETFs already show real demand for independent custody even where exchange trading stays separate from fund custody. Institutional capital will not accept trust us, here is a wallet balance as a custody standard. What it will accept is the same checklist that defines the framework: independent custody, audited key-management, proof of both assets and liabilities, clear legal entitlement, bankruptcy remoteness, transparent margin and liquidation rules, separated market makers, recovery and resolution planning, insurance and key-compromise disclosure, standardized customer-asset disclosure, sub-custodian transparency, and tested transfer procedures for distress. Regulation is one road to that checklist and market discipline is another, and the durable architecture will likely use both.

Conclusion

The lesson of traditional market structure is that the core functions must not fail together. Traditional finance has had severe failures, but most of them happened inside a layered system where the exchange, broker, custodian, clearing agency, settlement system, lender, and resolution process are distinct, so a shock in one place rarely became a loss everywhere. Centralized digital asset markets collapse those layers, and because digital assets are bearer-like and controlled through keys, that collapse turns custody into market structure. A compromised signer, an abused ledger, an affiliate loan, a token-collateral spiral, or a withdrawal run can each become a customer-asset event.

The record is mixed on how much customers ultimately recover and remarkably consistent on how the failures happen. Mt. Gox, Coincheck, Bitfinex, QuadrigaCX, Celsius, Voyager, BlockFi, Genesis, Gemini Earn, Three Arrows Capital, and Bybit differ in their facts and their outcomes, but they share one mechanism: a custody, credit, governance, or operational failure became a customer-asset loss because those functions lived in one place. The framework that answers this is functional isolation, and it reduces to a single rule. Custody, credit, trading, and settlement should not fail as one institution.



©2026 BitGo, Inc. (collectively with its parent, affiliates, and subsidiaries, "BitGo"). All rights reserved. BitGo Bank & Trust, National Association ("BitGo Bank & Trust") is a national trust bank chartered and regulated by the Office of the Comptroller of the Currency (OCC). BitGo Bank & Trust is a wholly-owned subsidiary of BitGo Holdings, Inc., a Delaware corporation headquartered in Sioux Falls, South Dakota. Other BitGo entities include BitGo, Inc. and BitGo Prime LLC, each of which is a separately operated affiliate of BitGo Bank & Trust. BitGo does not offer legal, tax, accounting, or investment advisory services. The information contained herein is for informational and marketing purposes only and should not be construed as legal, tax, or investment advice. Digital assets are subject to a high degree of risk, including the possible loss of the entire principal amount invested. Past performance and illustrative examples do not guarantee future results. BitGo Holdings, Inc., BitGo Bank & Trust, BitGo, Inc. and BitGo Prime LLC are not registered broker-dealers and are not members of the Securities Investor Protection Corporation ("SIPC") or the Financial Industry Regulatory Authority ("FINRA"). Digital assets held in custody are not guaranteed by BitGo and are not subject to the insurance protections of the Federal Deposit Insurance Corporation ("FDIC") or SIPC. This communication contains forward-looking statements. Forward-looking statements include all statements that are not historical facts. These statements may include words such as "aim," "anticipate," "assume," "believe," "contemplate," "continue," "could," "estimate," "expect," "forecast," "foreseeable," "guidance," "intend," "likely," "may," "objectives," "outlook," "plan," "potentially," "predict," "project," "seek," "should," "target," "will," "would," or variations of these terms and similar expressions. Such forward-looking statements are subject to various risks and uncertainties. Accordingly, there are or will be important factors that could cause actual outcomes or results to differ materially from those indicated in these statements. These factors include but are not limited to those described under "Risk Factors" in BitGo Holdings, Inc.'s most recent Annual Report on Form 10-K and other filings with the Securities and Exchange Commission ("SEC"), including any subsequently filed Quarterly Reports on Form 10-Q. These factors should not be construed as exhaustive and should be read in conjunction with the other cautionary statements that are included in BitGo Holdings, Inc.'s SEC filings. Although BitGo believes that the expectations reflected in its forward-looking statements are reasonable, it cannot guarantee future results. BitGo undertakes no obligation to publicly update or review any forward-looking statement, whether as a result of new information, future developments or otherwise, except as required by law. BitGo Holdings Inc.'s SEC filings are available at www.sec.gov. BitGo makes no representation that the information contained herein is appropriate for use in any jurisdiction where its distribution or use would be contrary to law or regulation or would subject BitGo or any of its affiliates to any registration or licensing requirements in such jurisdiction. Persons who access this information are responsible for complying with all applicable laws and regulations.

Sources

- Securities Exchange Act of 1934 and related exchange, broker-dealer, and clearing-agency provisions.
- SEC financial responsibility rules for broker-dealers, including Rules 15c3-1 and 15c3-3.
- SEC Regulation SCI materials and rules.
- SEC Rule 17Ad-22 clearing-agency standards.
- SIPC and U.S. Courts materials on SIPC broker-dealer liquidation.
- DTCC and DTC materials on custody, depository, and settlement services.
- SEC analysis of the July 8, 2015 NYSE trading suspension.
- SEC administrative materials on the January 2023 NYSE opening-auction disruption.
- SEC order and materials on the Nasdaq Facebook IPO systems failures.
- SEC order on the Knight Capital market-access failure.
- SEC staff report and congressional materials on the GameStop and Robinhood clearing-deposit stress.
- CFTC statements and enforcement materials on the MF Global customer-segregation failure.
- SEC complaints against Coinbase and Binance regarding combined exchange, broker, and clearing functions.
- SEC, DOJ, and bankruptcy materials on Celsius.
- SEC and New York Attorney General materials on Gemini Earn and Genesis.
- Bankruptcy materials on Voyager and BlockFi.
- DOJ materials on the Bitfinex hack and laundering case.
- FBI materials on the Bybit hack attribution.
- NYDFS virtual-currency custody guidance.
- SEC custody and safeguarding proposal materials, SAB 121 and SAB 122.
- Federal banking-agency and OCC crypto custody and safekeeping supervisory materials.
- Federal Register and congressional materials on stablecoin and digital asset market-structure legislation.
- FSB reports and recommendations on cryptoasset activities, global stablecoins, and multifunction cryptoasset intermediaries.
- IOSCO policy recommendations for crypto and digital asset markets and DeFi.
- BIS analysis of multifunction crypto intermediaries and crypto market vulnerabilities.
- ESMA and EU MiCA materials.
- UK FCA stablecoin and cryptoasset safeguarding consultation materials.
- Ontario Securities Commission report on QuadrigaCX.
- Mt. Gox trustee notices and related reporting on repayment timing.
- CoinGecko market-share, exchange-volume, reserve, and market-capitalization data.
- DefiLlama CEX transparency data.
- Glassnode exchange wallet-labeling limitations.
- Reuters reporting on Coincheck repayment, Voyager recovery, 3AC contagion, exchange concentration, and digital asset legislation.
- Chainalysis reporting on crypto theft and the Bybit hack.
- Binance and Bybit proof-of-reserves disclosures.
- Bitfinex disclosure on the 2016 hack and BFX token recovery.
- Gemini disclosure and Reuters reporting on Gemini Earn recovery.