# Tokenized Deposits, Stablecoins, and CBDCs: A Settlement-and-Custody Taxonomy for Regulated Institutions

ACM Global Tech

**Abstract**

"Digital money" is not one thing. A balance recorded on a distributed ledger may be a claim on a commercial bank, a claim on a non-bank issuer, or a claim on a central bank—three legally and operationally distinct instruments that share a transport rail but differ in who is liable, what stands behind the claim, how it settles, and how it is redeemed. Conflating them produces mispriced credit risk, misapplied regulation, and custody arrangements that fail under stress. This white paper supplies a precise taxonomy of the three principal forms—*tokenized deposits*, *stablecoins*, and *central bank digital currencies (CBDCs)*—organized around the dimensions a regulated institution actually underwrites: issuer and liability, backing, applicable regime in the United States and the European Union, settlement finality, custody model, redemption mechanics, privacy, and quantum-resistance posture. We then go deep on the two questions that most often decide an institutional deployment: custodial versus threshold (MPC) non-custodial custody, and the nature of settlement finality on a shared ledger. A decision guide maps each form to representative institutional use cases, and a closing section states ACM Global Tech's position: a single regulated, post-quantum ledger, built on Lux, Hanzo, and Zen, capable of issuing and servicing all three forms with MPC custody and FHE-based privacy.

## 1 Three Forms of Digital Money

The Bank for International Settlements frames the design space as a *unified ledger*: a common settlement venue on which tokenized central bank money, tokenized commercial bank deposits, and other tokenized claims coexist and settle atomically [1]. Within that frame, three issuer types produce three distinct liabilities. The distinctions are not cosmetic; they determine where credit risk sits and which body of law governs the claim.

### 1.1 Tokenized Deposit

A *tokenized deposit* is a commercial-bank deposit liability represented on a ledger. The holder's claim is on the issuing bank, exactly as with a conventional demand deposit; tokenization changes the *representation and transfer mechanism*, not the legal nature of the claim. Because the instrument remains a regulated bank deposit, it inherits the existing prudential apparatus: capital and liquidity requirements, deposit-insurance eligibility where applicable, and supervisory oversight of the issuing institution.

The decisive property of a tokenized deposit is that it preserves the *singleness of money*—the principle that a dollar of one bank's money exchanges at par with a dollar of any other bank's money and with central bank money [1]. Par exchange is not an emergent property of the token; it is maintained by interbank settlement in central bank reserves. On a unified ledger, a payment

between customers of two different banks is a simultaneous adjustment of two tokenized deposit balances settled against a movement of tokenized central bank money, so the payer's bank money and the payee's bank money remain mutually fungible at par. A tokenized deposit is therefore the on-ledger continuation of the two-tier monetary system rather than a departure from it.

### 1.2 Stablecoin

A *stablecoin* is a liability of a non-bank issuer, designed to hold a stable value (typically a 1:1 peg to a fiat currency) and backed by a reserve of assets held by or for the issuer. The holder's claim is on the issuer and, contractually, on the reserve—not on a bank's deposit base or on the central bank. The credit and liquidity risk of a stablecoin is the risk that the reserve is insufficient, illiquid, encumbered, or inaccessible at the moment of redemption.

Crucially, a stablecoin does *not* of itself guarantee singleness of money: two stablecoins, or a stablecoin and a bank deposit, trade at par only to the extent that arbitrage and redemption mechanisms hold, and that relationship can break under stress [1]. This is why stablecoins are regulated principally as a question of reserve quality, segregation, and redemption rights rather than as bank deposits. In the United States, the *GENIUS Act* establishes a federal framework for payment stablecoins, including reserve-backing and redemption requirements [3]. In the European Union, the Markets in Crypto-Assets Regulation (MiCA) governs "e-money tokens" and "asset-referenced tokens," imposing reserve, custody, and redemption obligations on issuers [2].

### 1.3 Central Bank Digital Currency (CBDC)

A *central bank digital currency* is a direct liability of the central bank in digital form—the digital analogue of physical cash or of reserve balances. As a central-bank claim it carries no issuer credit risk; it is the settlement asset of last resort. CBDCs divide into two operationally distinct classes:

**Wholesale CBDC.**
Restricted to financial institutions, used to settle interbank obligations and, on a unified ledger, to settle the interbank leg of tokenized-deposit payments. Wholesale CBDC is the on-ledger form of central bank reserves and is the mechanism by which par exchange and singleness of money are enforced [1].

**Retail CBDC.**
Available to the general public as a digital bearer or account claim on the central bank. Retail CBDC raises distinct questions of disintermediation, privacy, and the appropriate boundary between the central bank and commercial banks that wholesale designs largely avoid.

## 2 Comparison

Table 1 contrasts the three forms across the dimensions a regulated institution underwrites. The single most consequential row is *issuer / liability*, because it fixes where credit risk resides; every other dimension is downstream of it.

Two clarifications on the table. First, custody and quantum-resistance are *not* intrinsic to the instrument type: a stablecoin and a tokenized deposit issued on the same ledger inherit the same custody options and the same cryptographic posture. They appear as rows because they are first-order institutional concerns, but the answer is set by the platform, not the liability. Second, "settlement finality" means distinct things across the columns: for a tokenized deposit on a unified ledger it is the atomic, delivery-versus-payment settlement of the deposit leg against the reserve

| Dimension | Tokenized deposit | Stablecoin | CBDC |
|---|---|---|---|
| Issuer / liability | Commercial bank; bank deposit liability | Non-bank issuer; issuer liability | Central bank; central-bank liability |
| What backs it | Bank's balance sheet; settled in central bank reserves | Segregated reserve of fiat and/or high-quality liquid assets | Full faith of the central bank (no backing needed) |
| US regime | Existing bank law and prudential supervision | GENIUS Act (payment stablecoins) [3] | Pending; central-bank mandate, not yet authorized |
| EU regime (MiCA) | Bank deposit; outside MiCA token regime | E-money / asset-referenced token under MiCA [2] | Outside MiCA; central-bank instrument |
| Settlement finality | Atomic on unified ledger; par via reserve leg [1] | Ledger finality of issuer's chain; peg held by arbitrage | Definitive; central-bank money is the settlement asset |
| Custody model | Custodial or MPC non-custodial | Custodial or MPC non-custodial | Custodial or MPC non-custodial |
| Redemption | At par into reserves / other bank money | Contractual redemption against reserve [3, 2] | No redemption; it *is* base money |
| Privacy model | Bank-mediated; FHE/ZK selective disclosure feasible | Issuer-mediated; varies by chain | Policy choice (wholesale opaque; retail contested) |
| Quantum-resistance | Posture inherited from underlying ledger | Posture inherited from underlying ledger | Posture inherited from underlying ledger |

Table 1: Settlement-and-custody taxonomy of the three forms of digital money. "MPC non-custodial" denotes threshold custody in which no single party (including the venue) ever holds a complete key; see Section 3. Quantum-resistance is a property of the ledger and its signature scheme rather than of the instrument, and is therefore a platform decision.

leg; for a stablecoin it is the probabilistic-then-final settlement of the underlying chain, with par maintained only as long as redemption arbitrage functions [1].

# 3 Custody and Settlement Deep-Dive

For a regulated institution, the most important question about any of these instruments is not what backs it but *who can move it*. Two custody models dominate.

## 3.1 Custodial Custody

In the custodial model, a single operator holds the private keys that control the on-ledger balance. The operator can transfer assets unilaterally and is a single point of compromise: a breach of the operator's key store, an insider, or a legal compulsion against the operator can move customer assets. Custodial arrangements are familiar to regulators and can be operated compliantly, but they reintroduce precisely the concentration risk that a shared, programmable ledger is otherwise positioned to remove.

### 3.2 Threshold (MPC) Non-Custodial Custody

In threshold custody, the signing key is never assembled in one place. Secure multi-party computation (MPC) splits signing authority into $n$ shares distributed across independent parties, and a valid signature requires the cooperation of a threshold $t$ of them—a $t$-of-$n$ scheme, commonly 2-of-3. No party, at any time, holds a complete key; the key as a whole never exists in memory [6]. Authorization to move assets becomes a *policy* expressed as a quorum—for example, the asset owner plus one of several independent compliance signers—rather than possession of a secret by one operator.

The institutional consequence is precise and load-bearing: *the venue never holds keys.* A trading venue, an issuer, or a platform operator can provide matching, issuance, and servicing while being structurally incapable of unilaterally moving a customer's assets, because it controls at most one share below the threshold. This separates the operational role (running the venue) from the custodial role (controlling assets), which is exactly the separation that securities and money-transmission regimes ask for. It also narrows the blast radius of any single compromise: an attacker must simultaneously defeat $t$ independent parties rather than one key store [6].

### 3.3 Atomic Settlement and Finality

On a unified ledger, settlement of a payment or a securities trade is *atomic*: the two legs—two tokenized-deposit balances, or a tokenized security against tokenized money—either both complete or neither does, eliminating principal risk and Herstatt-style settlement risk [1]. Atomicity is what makes delivery-versus-payment and payment-versus-payment exact rather than best-effort. *Finality* is the guarantee that a settled transaction cannot be reversed; on a regulated ledger it should be deterministic (settled = final) rather than probabilistic. Threshold custody and atomic settlement compose cleanly: the quorum authorizes the transfer, the ledger settles both legs atomically, and finality attaches without any party having held unilateral control of the assets in between.

## 4 Decision Guide

The right instrument is the one whose liability structure and regime match the institution's mandate. Representative mappings:

**Credit union.**
A member-owned depository wants its members' balances to remain insured deposits and to retain its existing supervisory relationship. A **tokenized deposit** is the natural fit: members keep a claim on the institution, par exchange is preserved, and tokenization adds programmable, real-time transfer without changing the legal instrument. A stablecoin would move members' claims off the balance sheet and outside the deposit framework—rarely the goal.

**Community bank.**
Similar logic, with an added correspondent-banking dimension. A **tokenized deposit** on a unified ledger lets the bank settle interbank payments atomically against tokenized reserves, compressing correspondent latency while keeping the deposit relationship and prudential treatment intact [1].

**Broker-dealer.**
The priority is delivery-versus-payment settlement of securities against cash and unambiguous custody separation. A **tokenized deposit** (or wholesale CBDC where available) as the cash

leg, settled atomically against a tokenized security under **MPC non-custodial** custody, gives DvP with the venue structurally unable to touch client assets [6]. This is the configuration in which "the venue never holds keys" is most valuable.

**Corporate treasury.**
A non-bank corporate optimizing for 24/7 programmable settlement and broad counterparty reach may prefer a regulated **stablecoin** for always-on movement, while parking core operating balances in **tokenized deposits** for insured, par-stable holdings. The treasury's decision is a liquidity-versus-credit trade-off: stablecoin reach against deposit safety, made explicit by the taxonomy.

## 5 ACM's Stance

ACM Global Tech's position is that these three instruments should not require three incompatible platforms. ACM's platform is designed to issue and service all three forms—tokenized deposits, stablecoins, and CBDCs—on a single regulated, post-quantum ledger, with MPC threshold custody and FHE-based privacy as native properties of the ledger rather than bolt-ons [6, 7, 5]. Because custody and cryptographic posture are platform decisions (Table 1), unifying issuance lets an institution choose the liability that fits its mandate while inheriting one consistent custody and privacy model across all of them.

ACM is a Web3 Alliance (W3A) member and licenses this intellectual property to partners who resell and co-build it for regulated institutions. The platform pairs a real-time AI/ML AML engine with Stripe-class payment-service-provider and full banking-as-a-service capabilities, and is built on the Lux, Hanzo, and Zen stacks: Lux supplies the regulated post-quantum ledger and security-token semantics [4, 5], threshold custody follows the MPC custody design [6], and compliant privacy follows the threshold-FHE approach to selective disclosure [7]. These are stated as platform *capabilities*; they are not claims of specific production deployments.

## References


[1] Bank for International Settlements. *Blueprint for the future monetary system: improving the old, enabling the new*. BIS Annual Economic Report 2023, Chapter III. Bank for International Settlements, 2023. https://www.bis.org/publ/arpdf/ar2023e3.htm

[2] European Parliament and Council. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. Official Journal of the European Union, 2023. https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[3] United States Congress. *Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)*. Public law establishing a federal framework for payment stablecoins, including reserve-backing and redemption requirements.

[4] Z. Kelling. *The Lux Network: A Regulated, Post-Quantum Blockchain for Digital Securities, Real-World Assets, and Compliant Global Payments*. Lux Industries, Inc. Source: `lux:lux-whitepaper/lux-whitepaper.tex`.

[5] Z. Kelling. *Lux Security Token Standard: ERC-1400 on Post-Quantum EVM with MPC Custody*. Lux Partners. Source: `lux:lux-security-token-standard/lux-security-token-standard.tex`.

[6] Z. Kelling. *MPC Custody: Threshold Signing for Non-Custodial Regulated Asset Control*. Lux Partners. Source: `lux:mpc-custody/mpc-custody.tex`.

[7] Z. Kelling. *Threshold FHE for Compliant Privacy: Selective Disclosure on a Regulated Ledger*. Lux Partners. Source: `lux:threshold-fhe-compliance/threshold-fhe-compliance.tex`.