

CENTRAL BANK DIGITAL CURRENCY (CBDC).



A central bank digital currency turns monetary issuance into a distributed technical system — **the security question shifts from protecting data to protecting the integrity of money itself**, where a single compromised key can mean unauthorized currency, not just a leak.

- TIERED INTERMEDIATION
- ISSUANCE KEY CUSTODY
- OFFLINE DOUBLE-SPEND PREVENTION
- CROSS-BORDER INTEROPERABILITY

01 THE MECHANISM

Two-Tier Intermediation Model

Most CBDC designs keep commercial banks and payment providers in the loop rather than having the central bank hold every consumer account directly — **collapsing to a single-tier model turns the central bank into a retail bank overnight**, concentrating risk most central banks deliberately avoid.

Offline Double-Spend Prevention

Offline payments, made with no real-time ledger check, rely on tamper-resistant secure hardware inside the wallet to enforce a spend limit. **If that secure element is broken, an offline balance can be copied and spent twice** before the ledger ever reconciles.

Central Issuance Key Custody

The cryptographic keys authorizing new CBDC issuance are a single point of catastrophic failure for the currency itself — **a compromise can mint unauthorized money, not just leak data**, so issuance needs multi-party, HSM-backed control.

02 THE FLOW

The Intermediated, Tiered System

CONTAINED

1

The central bank issues CBDC under multi-party, HSM-backed key control and settles only with regulated intermediaries, never opening a direct consumer-facing surface at the central bank itself.

2

Wallets enforce tiered KYC and holding limits, so **a compromised wallet exposes only that customer's capped balance**, not the currency's integrity.

3

Offline transactions are bounded by secure-hardware spend limits and reconciled on reconnection, so **a cloned offline balance is capped and detectable**, not an unlimited forgery.

The Overcentralized, Unbounded System

EXPOSED

1

A single-tier design routes every consumer account and transaction through the central bank directly, turning routine retail-scale outages or breaches into **national payment-system incidents**.

2

Wallets with no enforced holding limits let intermediated deposits flow into CBDC en masse during a crisis, **accelerating a commercial bank run** rather than absorbing it.

3

Offline balances validated only by client-side software, with no secure hardware, can be **cloned and respent** before any ledger ever notices the duplication.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Tiered Architecture & Holding Limits	Keeps commercial banks and PSPs as the customer-facing layer and caps individual CBDC holdings, containing both breach blast radius and bank-run disintermediation risk.
Multi-Party Issuance Key Control	Splits the cryptographic authority to mint CBDC across multiple custodians and HSMs so no single compromised key can create unauthorized currency.
Tiered Privacy & AML Controls	Balances cash-like privacy for small transactions against full KYC/AML scrutiny for larger ones, since fully anonymous digital currency at national scale is not a workable compliance posture.
Offline Resilience & Secure Hardware	Uses tamper-resistant secure elements in wallets to enforce spend limits and prevent double-spending when a transaction can't reach the ledger in real time.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Central Bank Trust Alone, No Technical Controls	No	Institutional trust in the issuer doesn't prevent a technical compromise of issuance keys, wallets, or the settlement ledger itself.
Software-Only Offline Wallet Validation	No	Without tamper-resistant hardware, a rooted or cloned device can respend an offline balance before the ledger ever reconciles.
Single Custodian for Issuance Keys	No	Concentrates the ability to mint currency in one point of failure, whether that failure is a breach, an insider, or coercion.
Full Transaction-Level Anonymity	No	Meets a cash-like privacy goal but is incompatible with AML/CFT obligations at the scale of a national payment system.
Tiered Architecture + Multi-Party Issuance + Secure-Hardware Wallets + Tiered AML	Yes	Distributes trust and caps blast radius across the intermediation, issuance, wallet, and compliance layers at once.

CENTRAL BANK DIGITAL CURRENCY (CBDC).

ISSUE · INTERMEDIATE · SETTLE

05 PROGRAM OPERATIONS

Issuance key compromise is a currency-integrity event, not a data breach. Controls need to prevent unauthorized minting, not just unauthorized access to information.

CBDC is critical national infrastructure from day one. Availability and resilience requirements sit closer to power-grid uptime expectations than to a typical consumer banking app.

Holding limits are a security control, not just a monetary-policy lever. They cap how much value a single compromised wallet or account can expose.

Cross-border CBDC interoperability multiplies interconnection risk. Linking multiple national systems, as in BIS multi-CBDC pilots, recreates the correspondent-banking trust problem in new technical form.

06 CONTROL MAPPING

BIS CBDC SECURITY GUIDANCE

Bank for International Settlements guidance on CBDC architecture, cyber resilience, and multi-CBDC interoperability from its Innovation Hub pilots.

IMF CBDC VIRTUAL HANDBOOK

IMF technical guidance for central banks on legal, technical, and policy considerations across CBDC design choices.

ISO 20022

Structured payment messaging standard increasingly used to carry CBDC transaction data alongside traditional payment rails.

NIST POST-QUANTUM CRYPTOGRAPHY STANDARDS

Quantum-resistant algorithm standards relevant to any CBDC issuance and signing infrastructure expected to stay secure for decades.

07 WHAT THIS DOES NOT SOLVE

Monetary Policy & Disintermediation Debate
Holding limits reduce security blast radius but don't resolve the underlying policy question of how much commercial banking should be displaced.

Consumer Device Security
A secure CBDC wallet architecture still depends on the security of the consumer's own phone or hardware token, which sits outside the central bank's control.

Cross-Border Regulatory Harmonization
Interoperable multi-CBDC settlement doesn't by itself resolve differing AML, sanctions, and privacy regimes between connected jurisdictions.

Merchant & Endpoint Acceptance Fraud
A cryptographically sound CBDC transaction can still be obtained through social engineering or merchant-side fraud at the point of acceptance.

08 MYTHS VS. REALITY

MYTH
“CBDC is just cryptocurrency issued by a government.”

REALITY
Most CBDC designs are centrally issued and controlled, often without a public blockchain at all — the resemblance to cryptocurrency is mostly the word “digital,” not the trust model.

MYTH
“A two-tier system is less secure because it adds intermediaries.”

REALITY
Intermediation contains breach and outage blast radius to one institution's customers instead of exposing the central bank's core system directly to every retail transaction.

MYTH
“Offline CBDC payments are as secure as cash because there's no network to attack.”

REALITY
Removing the network removes real-time validation too — security shifts entirely onto the wallet's secure hardware, the sole line of defense against double-spending.

MYTH
“Full transaction privacy is achievable without compromising AML enforcement.”

REALITY
Every current major CBDC design trades some privacy for AML compliance above certain transaction values; full cash-like anonymity at scale has not shipped anywhere.

MYTH
“CBDC security is primarily a cryptography problem.”

REALITY
Cryptography protects individual transactions, but issuance key governance, intermediation architecture, and wallet endpoint security determine whether the system holds up as a whole.

09 SPEAK THE PROGRAM — KEY TERMS

TWO-TIER (INTERMEDIATED) CBDC
An architecture where the central bank issues currency but commercial banks or PSPs manage customer accounts and wallets, preserving the existing banking relationship layer.

DIRECT (SINGLE-TIER) CBDC
An architecture where the central bank operates consumer-facing accounts itself, largely avoided in current designs due to operational and security concentration risk.

HOLDING LIMITS
Caps on how much CBDC an individual account or wallet can hold, used to bound both bank-run disintermediation risk and breach exposure.

TIERED KYC / PRIVACY
A design pattern giving lighter identity checks and more privacy to small transactions, with fuller KYC and monitoring above defined thresholds.

SECURE ELEMENT (WALLET HARDWARE)
Tamper-resistant hardware inside a device that enforces offline spend limits and prevents balance duplication when a wallet can't reach the ledger.

MULTI-CBDC INTEROPERABILITY
Technical arrangements, such as BIS's Project mBridge, letting different countries' CBDC systems settle transactions across borders, extending trust relationships between issuers.