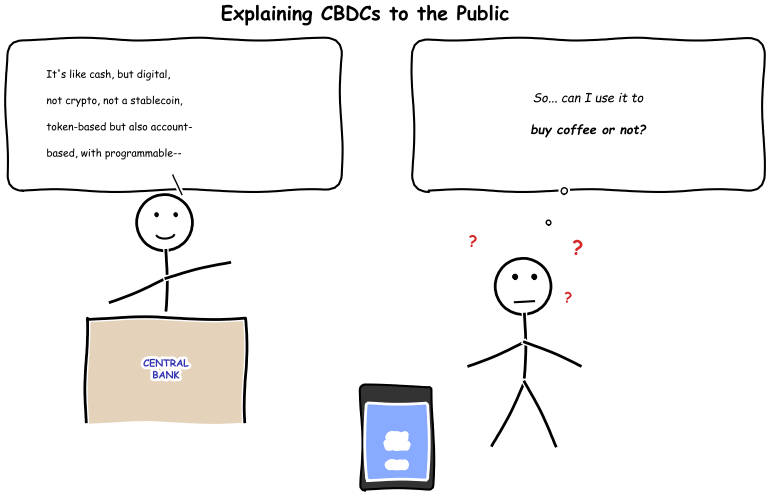
Lesson 6.4: Next-Generation Infrastructure

Module 6: The Infrastructure Problem

Prof. Dr. Joerg Osterrieder



The technology is ready. The explanation isn't.

Learning Objectives

After this lesson you will be able to:

1. **Explain** the difference between retail and wholesale CBDCs and their design tradeoffs [Understand]
2. **Compare** account-based vs. token-based CBDC architectures and their privacy implications [Analyze]
3. **Distinguish** custodial, non-custodial, and MPC-based digital wallet models [Analyze]
4. **Describe** the mechanics of real-world asset (RWA) tokenization and its settlement advantages [Understand]
5. **Evaluate** programmable money as a coordination mechanism for conditional payments [Evaluate]
6. **Analyze** Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) as infrastructure for digital finance [Analyze]

Bloom's levels: Understand (1,4), Analyze (2,3,6), Evaluate (5).

From Open APIs to Rebuilt Rails

Lesson 6.3 – APIs and Open Banking:

- APIs opened the financial system to third parties
- PSD2 and Open Banking mandated data sharing
- Embedded finance placed banking inside non-bank apps
- But the underlying rails remain 40+ years old

Lesson 6.4 – Next-Gen Infrastructure:

- CBDCs replace commercial bank money with central bank digital currency
- Tokenization converts real-world assets into on-chain representations
- Programmable money automates conditional payments
- Self-Sovereign Identity gives users control over digital credentials

APIs opened the system. CBDCs and tokenization may rebuild it from scratch.

Next-generation infrastructure does not patch existing rails — it proposes entirely new ones. This lesson examines what those new rails look like.

What Is a Central Bank Digital Currency (CBDC)?

Definition: A **CBDC** is a digital form of central bank money — a liability of the central bank — available to the general public (retail CBDC) or to financial institutions (wholesale CBDC).

What a CBDC is:

- Legal tender issued by the central bank
- Risk-free: no credit risk (unlike bank deposits)
- Digital-native: not a digitized version of physical cash
- Programmable (optionally): conditional transfers possible

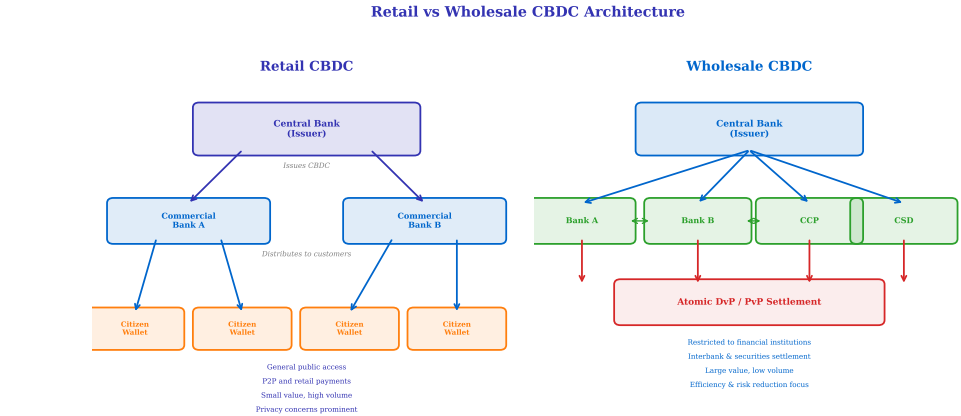
What a CBDC is not:

- Not a cryptocurrency (centrally issued and controlled)
- Not a stablecoin (not backed by reserves, *is* the reserve)
- Not a replacement for bank deposits (in most designs)
- Not blockchain-dependent (many use centralized ledgers)

Global status (as of 2025): Over 130 countries exploring CBDCs. The Bahamas (Sand Dollar), Nigeria (eNaira), and Jamaica (JAM-DEX) have launched retail CBDCs. China's e-CNY pilot covers 260+ million wallets.

A CBDC is a policy instrument, not just a technology. Central banks design CBDCs to achieve specific monetary policy and financial stability goals.

Retail vs. Wholesale CBDCs



- **What you see:** Left panel shows retail CBDC — central bank issues to commercial banks, who distribute to citizens. Right panel shows wholesale CBDC — direct interbank settlement with central bank
- **Key pattern:** Retail = general public access, P2P payments; Wholesale = large-value transfers, faster interbank settlement, lower operational costs
- **Takeaway:** Retail CBDCs raise policy questions (bank disintermediation, privacy); wholesale CBDCs are technically simpler and less

Account-Based vs. Token-Based CBDC

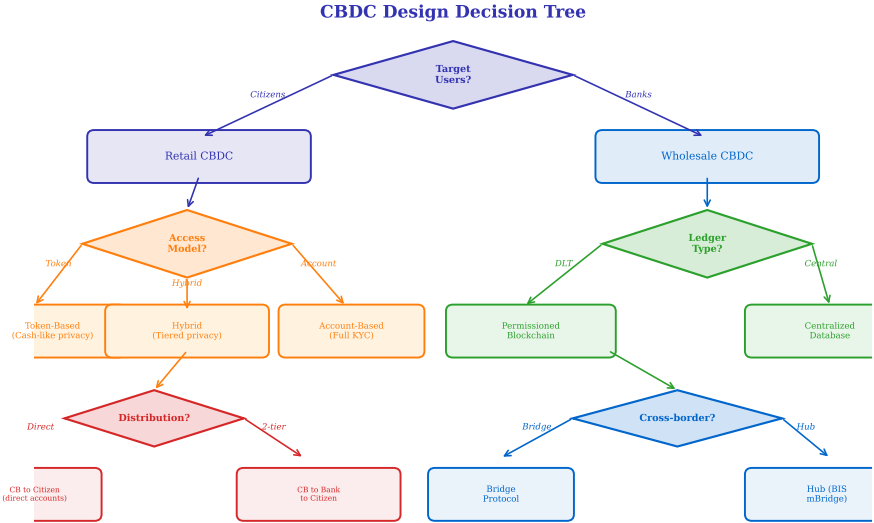
Definition: The **access model** determines how ownership of CBDC units is verified — by identity (account-based) or by possession of a cryptographic token (token-based).

Dimension	Account-Based	Token-Based
Identity	Transaction requires identity verification	Transaction requires proof of possession (private key)
Analogy	Like a bank account	Like physical cash
Privacy	Low: all transactions linked to identity	Higher: can be pseudonymous or anonymous
Offline use	Difficult without central ledger access	Possible with hardware tokens
AML/KYC	Built-in (identity required)	Requires additional mechanisms
Double-spend	Prevented by ledger reconciliation	Prevented by cryptographic proofs

Hybrid approaches: The ECB's digital euro design proposes tiered privacy — small offline transactions with limited identity checks, larger online transactions with full KYC.

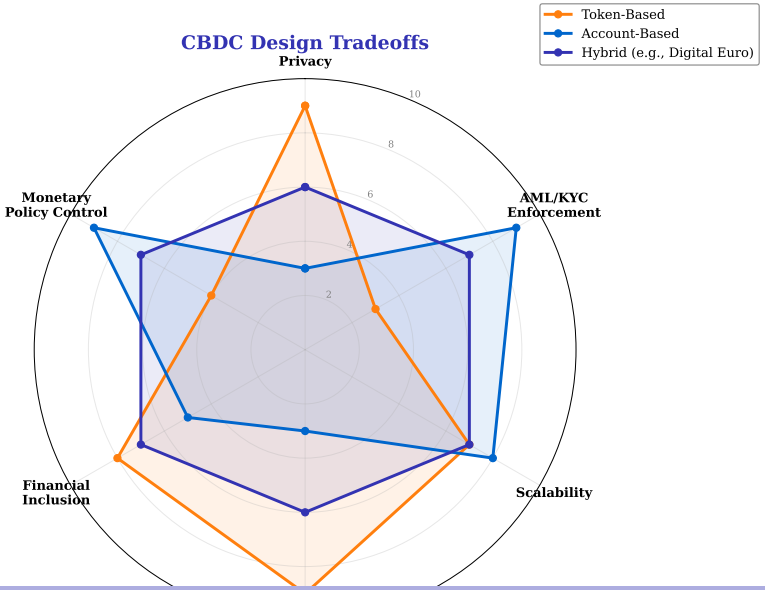
The account vs. token choice is fundamentally a tradeoff between surveillance and privacy. Most designs converge on hybrid solutions.

CBDC Design Decision Tree



- **What you see:** Decision tree with 4 key questions — Retail or Wholesale? (if Retail): Account-based or Token-based? Centralized

CBDC Design Tradeoffs



Case Study: The Digital Euro

The ECB's digital euro project: A retail CBDC for the euro area. preparation phase extended to Oct 2025; decision on next phase ongoing, earliest launch 2027–2028 (*ECB Governing Council communications; BIS CBDC tracker*, 2026).

Key design choices:

- **Distribution:** Two-tier model — ECB issues, commercial banks distribute
- **Holding limit:** Proposed cap of €3,000 per person to prevent bank disintermediation
- **Privacy:** Offline payments with "cash-like" privacy for small amounts
- **Technology:** Centralized ledger (not blockchain-based)

Policy motivations:

- **Monetary sovereignty:** Counter the rise of private stablecoins and foreign CBDCs — note the US GENIUS Act (signed July 2025) (*US Congress; OCC stablecoin charter framework*, 2025) now sets a federal stablecoin regime, accelerating EU urgency
- **Financial inclusion:** Provide a digital payment option for the unbanked
- **Payment efficiency:** Create a pan-European instant payment rail
- **Strategic autonomy:** Reduce dependence on non-European card networks (Visa, Mastercard)

Open question: Will consumers adopt a CBDC with a €3,000 cap when existing bank accounts offer higher balances and deposit insurance?

The digital euro is as much a geopolitical project as a technical one. It reflects the ECB's desire to maintain the euro's role in digital payments.

What Is a Digital Wallet?

Definition: A **digital wallet** is software (or hardware) that stores, manages, and transacts digital assets — including CBDCs, tokens, credentials, and keys — on behalf of a user.

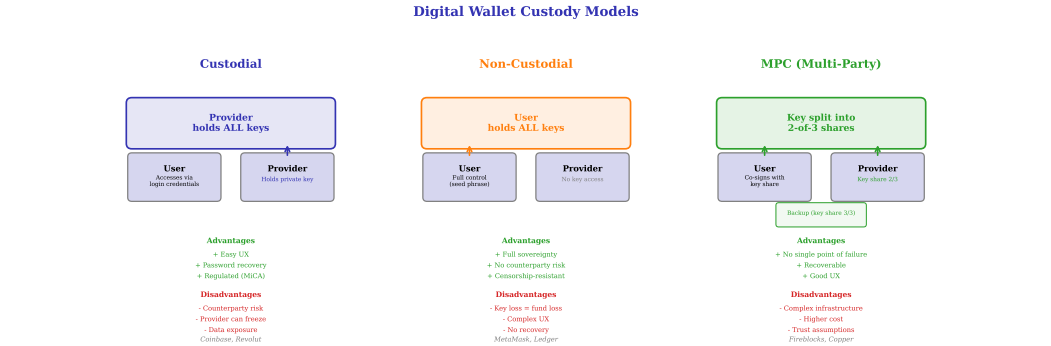
Types of digital wallets:

1. **Payment wallets:** Store payment credentials (Apple Pay, Google Pay) — proxy for existing bank accounts
2. **Crypto wallets:** Store private keys for blockchain-based assets (MetaMask, Ledger)
3. **CBDC wallets:** Issued or approved by central banks to hold digital currency
4. **Identity wallets:** Store verifiable credentials (EU Digital Identity Wallet under eIDAS 2.0)
5. **Multi-asset wallets:** Converge all of the above into a single interface

Key insight: The wallet is becoming the *universal interface* between individuals and the digital financial system — replacing cards, accounts, and identity documents with a single app.

The EU Digital Identity Wallet regulation (electronic Identification, Authentication and trust Services (eIDAS) 2.0) mandates that all EU member states offer a digital identity wallet to citizens by 2026.

Wallet Custody Models



- **What you see:** Three custody models — Custodial (provider holds keys, UX easy but trust required), Non-Custodial (user holds keys, no trust needed but risk of loss), MPC (keys split across parties, balanced approach)
- **Key pattern:** Custodial = bank-like (Coinbase, Revolut); Non-Custodial = "not your keys not your coins" (MetaMask, Ledger); MPC = institutional standard (Fireblocks, Copper)
- **Takeaway:** Custody determines regulatory treatment — custodial wallets require licenses (Markets in Crypto-Assets Regulation (MiCA)), non-custodial wallets are unregulated (for now)

Custody is the central design decision: who holds the private keys? Each model implies different security, usability, and regulatory treatment.

Custodial vs. Non-Custodial Wallets

Dimension	Custodial	Non-Custodial
Key management	Provider holds private keys	User holds private keys
Recovery	Password reset via provider	Seed phrase (12–24 words); if lost, funds are irrecoverable
Regulation	Provider is regulated (MiCA, bank license)	User is self-sovereign; no intermediary to regulate
Counterparty risk	Yes (exchange hack, insolvency)	No (user controls funds directly)
UX complexity	Low (like a bank app)	Higher (must manage keys, gas fees)
Examples	Coinbase, Revolut, bank CBDC wallets	MetaMask, Ledger, Trezor

Emerging middle ground — Multi-Party Computation (MPC) wallets:

- **MPC:** The private key is split into shares held by multiple parties (user, provider, backup)
- No single party can sign alone → reduces both custodial risk and key-loss risk
- Used by institutional custody providers: Fireblocks, Copper, Fordefi

"Not your keys, not your coins" was the crypto mantra. MPC wallets offer a pragmatic compromise between security and usability.

What Is Real-World Asset (RWA) Tokenization?

Definition: RWA tokenization is the process of representing ownership rights to real-world assets — bonds, equities, real estate, commodities — as digital tokens on a distributed ledger.

What gets tokenized:

- **Bonds:** Goldman Sachs, EIB, and Siemens have issued tokenized bonds; **SIX Digital Exchange (SDX)** runs the world's first regulated tokenised-bond CSD in Switzerland (City of Lugano CHF 100M bond 2023; UBS digital bond 2022)
- **Real estate:** Fractional ownership via tokens (e.g., RealT)
- **Private equity:** Tokenized fund shares with automated distributions
- **Commodities:** Gold-backed tokens (Paxos Gold, Tether Gold)
- **Treasury bills:** On-chain T-bills (Ondo Finance, Franklin Templeton)

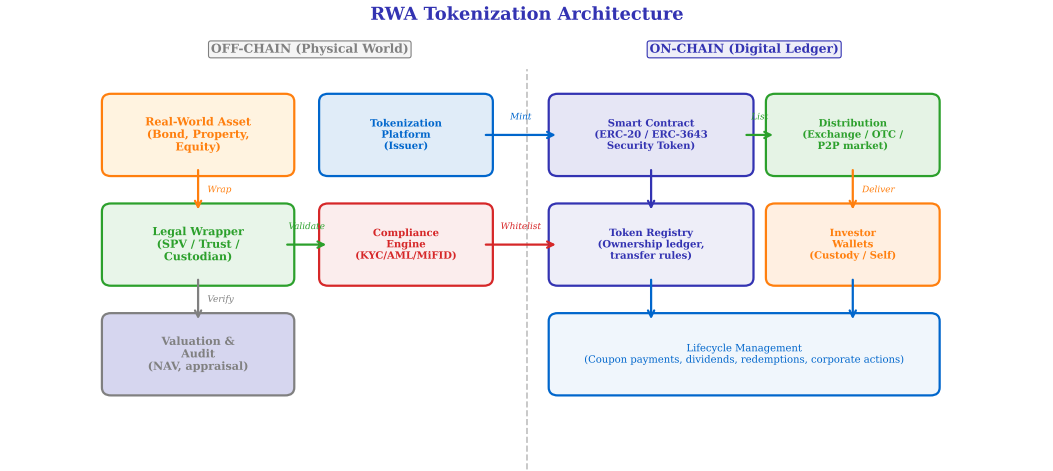
SIX SDX operates as a FINMA-licensed exchange + CSD on the DLT-Act framework; deeper coverage in the standalone `lecture_tokenization_revolution.tex`.

Why tokenize:

- **24/7 settlement:** No waiting for T+1 or T+2 cycles
- **Fractional ownership:** Divide a $100M bond into $100 units
- **Programmability:** Auto-execute coupon payments, dividends
- **Transparency:** Ownership visible on-chain in real-time
- **Global access:** Permissioned tokens tradeable across borders

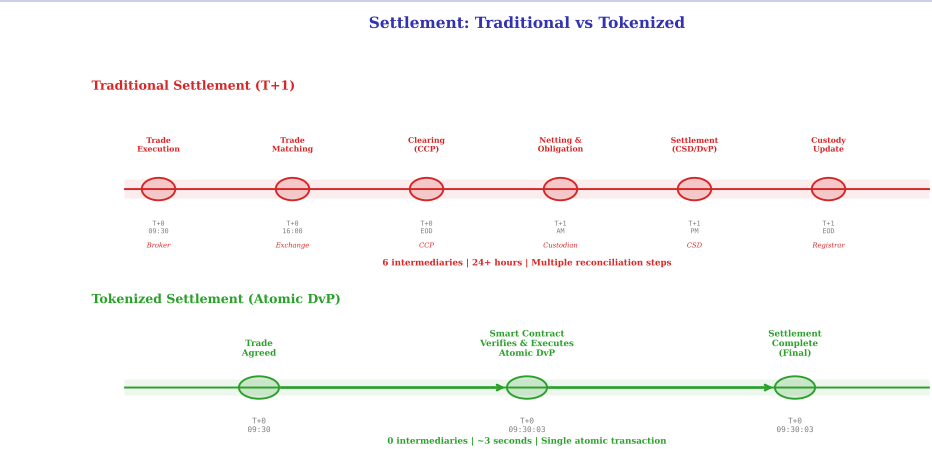
Market size: €15.25B tokenized RWA TVL (on-chain stablecoins) as of €1Dec 2023 (source: 2026); 2030 forecast

RWA Tokenization Architecture



- **What you see:** Four-layer architecture — off-chain asset (bottom), legal wrapper (SPV/trust), tokenization layer (smart contract), and on-chain token (top). Arrows show how legal ownership connects to digital representation

Tokenized vs. Traditional Settlement



Tokenized settlement compresses T+1 into seconds, freeing capital and eliminating reconciliation.

- **What you see:** Side-by-side comparison showing Traditional (T+2, multi-day process with trade matching, netting, settlement) vs. Tokenized (atomic DvP, seconds, single on-chain transaction)
- **Key pattern:** Traditional settlement requires intermediaries (CCP, CSD, custodians) and takes 2+ days; tokenized settlement is

The Unified Ledger Concept (BIS)

Definition: The **unified ledger** is a concept proposed by the Bank for International Settlements (BIS) in which CBDCs, tokenized deposits, and tokenized assets coexist on a single programmable platform.

Architecture layers:

1. **Data layer:** All financial assets represented as tokens on a shared ledger
2. **Execution layer:** Smart contracts enforce business logic (settlement, compliance)
3. **Governance layer:** Central banks set rules; commercial banks operate within them
4. **Privacy layer:** Partitioned data access — each participant sees only what they are authorized to see

Key innovation — atomic settlement:

- **Delivery-vs-Payment (DvP):** Asset and payment transfer simultaneously in a single atomic transaction
- **Payment-vs-Payment (PvP):** Two currencies exchange simultaneously (eliminates Herstatt risk)
- Eliminates the need for central counterparties (CCPs) and custodian chains for many transaction types

---

The BIS unified ledger is a vision, not a product. It represents the direction of travel for central bank infrastructure modernization.

What Is Programmable Money?

Definition: Programmable money is digital currency with embedded logic that can execute conditional transfers automatically — "money that knows the rules."

Types of programmability:

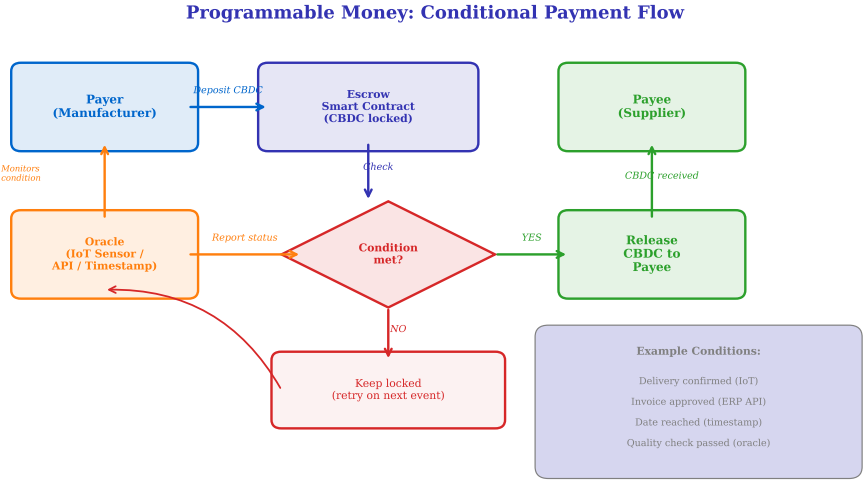
1. **Programmable payments:** Logic attached to the payment instruction, not the money itself (e.g., standing orders, escrow release)
2. **Programmable money:** Logic embedded in the currency unit — the money itself carries conditions (e.g., "can only be spent at pharmacies" or "expires after 90 days")
3. **Purpose-bound money (PBM):** A wrapper around CBDC units that imposes spending constraints, proposed by the Monetary Authority of Singapore (MAS)

Financial use cases:

- **Supply chain finance:** Payment triggers automatically when IoT sensors confirm delivery
- **Government disbursements:** Social welfare payments restricted to essential goods
- **Corporate treasury:** Automated tax withholding at the point of transaction
- **Escrow automation:** M&A milestone payments released when conditions are verified on-chain
- **Know Your Customer (KYC) and Anti-Money Laundering (AML):** Automated compliance checks embedded in payment flows

Programmable money raises profound questions: Should money have "opinions" about how it can be spent? The technical capability exists; the policy debate is ongoing.

Programmable Money: Conditional Payment Flow



- **What you see:** Flow diagram showing traditional payment (manual verification, escrow agent) vs. programmable payment (smart

Risks and Controversies of Programmable Money

Technical risks:

- **Smart contract bugs:** Errors in payment logic can lock or misdirect funds
- **Oracle dependency:** External data feeds (IoT, APIs) can be manipulated
- **Composability risk:** Complex chains of conditional payments may fail unpredictably
- **Irrevocability:** Automated execution leaves no room for human judgment

Societal risks:

- **Financial surveillance:** Governments could track and restrict every transaction
- **Spending restrictions:** "Money that expires" or "money only for approved vendors" limits individual freedom
- **Social credit integration:** CBDCs could be linked to behavioral scoring systems
- **Exclusion:** Citizens without compatible wallets may be locked out

Design principle: The ECB has stated that the digital euro will *not* be programmable money (no expiry, no restrictions on where it can be spent), but *will* support programmable payments (automated triggers).

The line between "useful automation" and "financial control" depends entirely on who writes the rules and who can change them.

What Is Self-Sovereign Identity (SSI)?

Definition: Self-Sovereign Identity (SSI) is a model where individuals own, control, and share their digital identity credentials without relying on a centralized authority.

Core components:

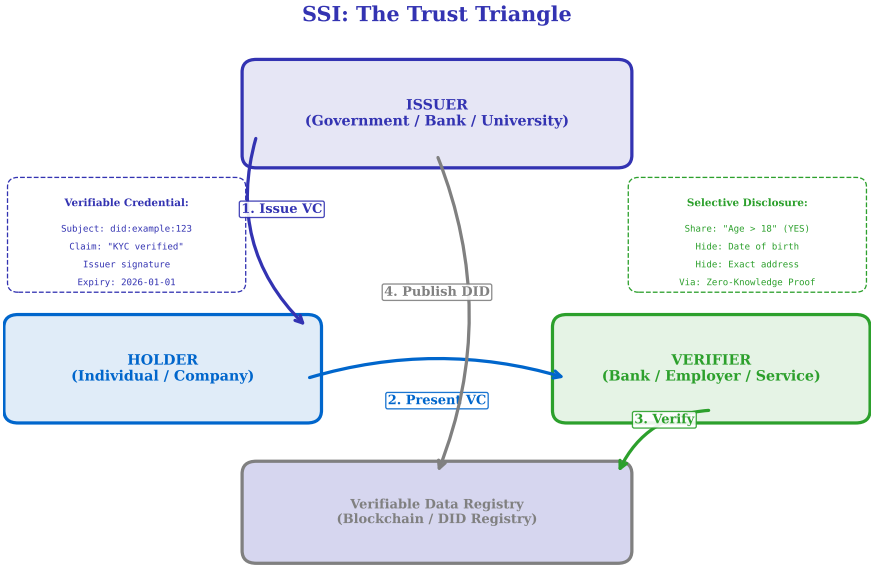
1. **Decentralized Identifiers (DIDs):** Globally unique identifiers controlled by the subject, not a central registry. Format: `did:example:123abc`
2. **Verifiable Credentials (VCs):** Digital equivalents of physical documents (passport, diploma, bank statement) signed by an issuer
3. **Identity Wallet:** Software that stores VCs and presents them selectively to verifiers
4. **Verifiable Data Registry:** A shared ledger (often blockchain) that stores DID documents and credential schemas

Key property — selective disclosure:

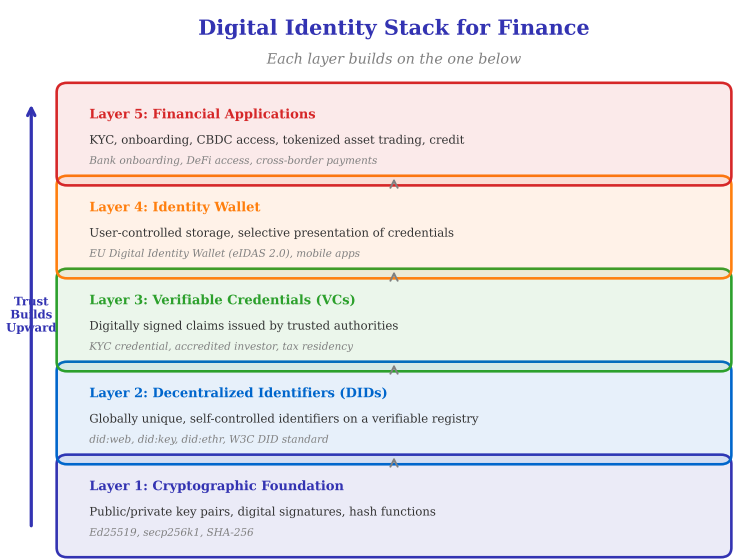
- Prove "I am over 18" without revealing your date of birth
- Prove "I have a bank account with balance $>$ €10,000" without revealing the exact balance
- Zero-knowledge proofs enable cryptographic verification without data exposure

---

SSI inverts the identity model: instead of institutions holding your data and sharing it, you hold your data and share only what is needed.



The Digital Identity Stack for Finance



SSI Applications in Financial Services

Use Case	Current Process	SSI-Enabled Process
KYC onboarding	Customer submits documents to each bank separately	Customer shares a verified KYC credential once; banks verify cryptographically
Cross-border identity	Passport scans, notarized translations	DID-based credential recognized across jurisdictions
Credit scoring	Central bureaus hold data; consumers have limited control	Consumer holds verifiable credit credential; shares selectively
Corporate identity	Company registers with each exchange, custodian, counterparty	Legal Entity Identifier (LEI) as a verifiable credential
Regulatory reporting	Banks submit data to each regulator separately	Regulator verifies on-chain attestations without data duplication

EU regulatory driver: eIDAS 2.0 mandates EU Digital Identity Wallets, creating the infrastructure for SSI in all member states.

SSI in finance reduces KYC costs (currently $60–500M/year for large banks) by eliminating redundant identity verification.

Convergence: CBDC + Tokenization + Identity

The three pillars of next-generation financial infrastructure are converging:

1. **CBDC (the money):** Digital central bank money as the settlement asset
2. **RWA tokenization (the assets):** Securities, real estate, and commodities as programmable tokens
3. **SSI/DID (the identity):** Verifiable digital identity as the access credential

Convergence example — tokenized bond purchase:

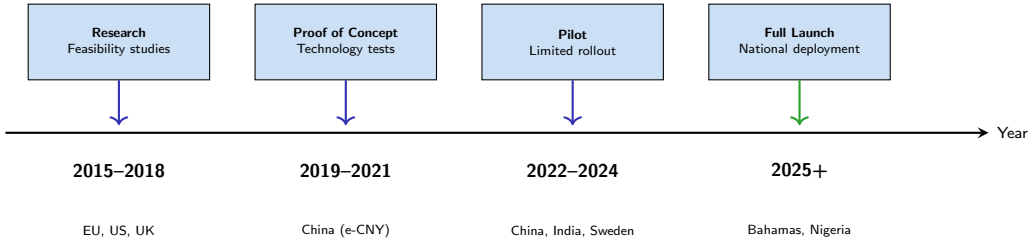
1. Investor authenticates with DID-based verifiable credential (accredited investor status)
2. Smart contract verifies credential against compliance rules
3. Investor transfers CBDC to the bond issuer's address
4. Tokenized bond transfers to the investor's wallet
5. Settlement is atomic (DvP), instant, and fully auditable
6. Coupon payments auto-execute to the wallet holding the bond token

No intermediaries needed for: identity verification, payment clearing, custody, coupon distribution.

Reality check: This is target architecture — no jurisdiction has deployed the full CBDC + tokenization + DID stack end-to-end (*BIS Innovation Hub; SNB Project Helvetia III remains the closest operational wholesale DvP*, 2026). Helvetia III (wholesale CBDC on SDX) and Project Agora are the closest live building blocks.

The convergence of CBDC, tokenization, and SSI represents a potential paradigm shift: from intermediated finance to programmable, self-executing finance.

CBDC Evolution Timeline: From Research to Launch



Observation: Most major economies are in the "Pilot" phase (2022–2024). Full nationwide CBDC launches remain rare (only small island nations and Nigeria as of 2025).

CBDC development follows a 5–10 year arc from initial research to full deployment. The pilot phase is where most central banks are today.

Global CBDC Landscape (2025)

Central banks worldwide are at different stages of CBDC exploration:

Stage	Countries/Regions	Status
Launched	Bahamas, Nigeria, Jamaica, Eastern Caribbean	Live retail CBDCs with lim
Advanced pilot	China (e-CNY), India (e-Rupee), Sweden (e-Krona)	Large-scale testing with mi
Preparation	EU (digital euro), UK, Brazil, Japan, Australia	Active design and prototyp
Research	USA (FedNow is *not* a CBDC), Canada, South Korea	Exploring feasibility and po
Cautious/opposed	Some jurisdictions concerned about privacy and bank disintermediation	Policy debate ongoing

Key observation: No major economy has a CBDC at scale yet. China's e-CNY is the most advanced, but adoption remains a small fraction of total payments.

The CBDC race is less about who launches first and more about who designs the most useful and widely adopted system.

Challenges and Open Questions

Technical challenges:

- **Scalability:** Can CBDC infrastructure handle 100,000+ Transactions Per Second (TPS) (peak retail volume)?
- **Interoperability:** How do CBDCs from different countries interact?
- **Offline payments:** How to prevent double-spending without network access?
- **Quantum threat:** Current cryptography may be broken by quantum computers in 10–15 years

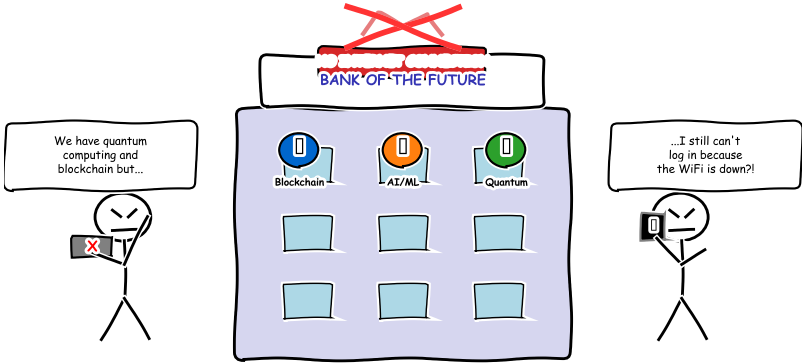
Policy challenges:

- **Bank disintermediation:** Will CBDC deposits drain commercial bank funding?
- **Privacy vs. AML:** How to balance user privacy with anti-money-laundering requirements?
- **Geopolitical fragmentation:** Will CBDCs reinforce or undermine the dollar's reserve status?
- **Digital divide:** How to ensure access for the elderly, rural, and unbanked populations?

Cross-border interoperability projects: mBridge (BIS + China, UAE, Thailand, Hong Kong), Project Icebreaker (BIS + Israel, Norway, Sweden), Project Dunbar (BIS + Singapore, Australia, Malaysia, South Africa).

The hardest problems in CBDC design are not technical — they are political: privacy, control, and the future role of commercial banks.

One Last Thought...



Next-gen infrastructure: Quantum-ready, AI-powered, blockchain-secured... WiFi: optional

Sometimes the best way to remember a concept is to laugh about it.

Key Takeaways

1. **CBDCs** are digital central bank money. Retail CBDCs serve citizens; wholesale CBDCs optimize interbank settlement. Over 130 countries are exploring them
2. **Account-based vs. token-based** is the fundamental privacy tradeoff: identity-linked surveillance vs. cash-like anonymity. Most designs converge on hybrids
3. **Digital wallets** are becoming the universal interface for money, assets, and identity. Custody models (custodial, non-custodial, MPC) determine who holds the keys
4. **RWA tokenization** wraps real-world assets in digital tokens for 24/7 settlement, fractional ownership, and programmable distributions
5. **Programmable money** embeds spending logic in currency units. The distinction between programmable money and programmable payments is critical for civil liberties
6. **Self-Sovereign Identity (SSI)** gives users control over digital credentials. DIDs and verifiable credentials can eliminate redundant KYC and enable selective disclosure
7. **Convergence** of CBDC + tokenization + SSI points toward a future of atomic, self-executing financial transactions without intermediaries

---

Next-generation infrastructure is not incremental improvement — it is a fundamental rearchitecting of how money, assets, and identity flow through the financial system.

Summary / Next Lesson Preview

This lesson:

- Compared retail and wholesale CBDC designs and their policy tradeoffs
- Analyzed account-based vs. token-based architectures and privacy implications
- Distinguished custodial, non-custodial, and MPC wallet models
- Explained RWA tokenization mechanics and settlement advantages
- Evaluated programmable money capabilities and civil liberty concerns
- Described SSI/DID infrastructure and its financial services applications

What comes next in Module 7 – The Compliance Problem:

- How do regulators keep up with the pace of financial innovation?
- RegTech: technology-enabled compliance and supervisory technology (SupTech)
- The EU AI Act, MiCA, DORA, and the evolving global regulatory landscape
- Balancing innovation incentives with consumer protection and systemic stability

---

We have now covered the full infrastructure stack: legacy systems, payments, APIs, and next-gen rails. Module 7 asks: who governs all of this?

Self-Check: Next-Gen Infrastructure

Attempt these before turning the page.

1. [Understand] Contrast retail CBDC from wholesale CBDC. Which is further developed globally, and why?
2. [Apply] A tokenised sovereign bond settles T+0 instead of T+2. For a $10B daily volume, estimate the intraday liquidity freed. Assume average funding cost 4.5% on the interim float.
3. [Evaluate] China's e-CNY has 260M+ wallets but low active use. Is this successful adoption? State your criterion explicitly.

Solutions hidden unless `\solutionstrue` is set before compiling.