Exercises: Lesson 6.4 – Next-Generation Infrastructure

Module 6: The Infrastructure Problem

Prof. Dr. Joerg Osterrieder

Exercise 1: CBDC Design Choices for a European Country

Scenario: You are advising a mid-size European country's central bank on launching a retail CBDC. The country has a well-banked population (98% bank account penetration), a mature instant payment system, and strong privacy expectations.

Tasks:

1. Choose between account-based, token-based, or hybrid access model. Justify your choice considering the population's privacy expectations and existing AML regulations.
2. Propose a holding limit. Explain the tradeoff between financial inclusion and bank disintermediation at your chosen limit.
3. Should the CBDC support offline payments? Analyze the technical challenge of preventing double-spending in offline mode.
4. Design the distribution model: direct (central bank $\rightarrow$ citizen) or two-tier (central bank $\rightarrow$ commercial bank $\rightarrow$ citizen). What role do commercial banks play in each model?
5. The country is an EU member. How does the digital euro project affect your recommendation? Should the country wait for the digital euro or proceed independently?

Exercise 2: Wallet Custody Model Comparison

Scenario: A neobank is launching a digital asset service that allows customers to hold both CBDC and tokenized securities. The compliance team requires regulatory clarity; the product team wants the best UX; the security team worries about key management.

Tasks:

a. Complete a comparison matrix for three custody models (custodial, non-custodial, MPC) across five dimensions: security, UX, regulatory compliance, recovery options, and cost.

b. The neobank's average customer is 28 years old, uses mobile banking daily, and has no experience with seed phrases. Which custody model do you recommend and why?

c. Design a key recovery flow for your recommended model. What happens if the customer loses their phone? What if the neobank goes bankrupt?

d. Under MiCA regulation, custodial crypto-asset service providers must hold a license. How does this affect the neobank's choice?

Exercise 3: RWA Tokenization Business Case

Scenario: A real estate investment firm owns a portfolio of 20 commercial properties worth €500 million total. The firm wants to tokenize the portfolio to attract smaller investors.

Given data:

- Current minimum investment: €5,000,000 (limited to institutional investors)
- Proposed tokenized minimum: €100 per token
- Annual rental yield: 5.2%
- Tokenization platform cost: €2M setup + €400K/year operations
- Legal structuring (SPV, compliance): €800K one-time
- Expected new investor inflow: €50M in Year 1

Tasks:

a) Calculate the total Year 1 cost of tokenization.

b) Calculate the additional annual rental income from the €50M new investment.

c) What is the payback period for the tokenization investment?

d) Identify three legal risks specific to tokenized real estate (e.g., what happens if the SPV is challenged in court?).

Exercise 4: Designing Programmable Money for Supply Chain Finance

Scenario: A multinational manufacturer pays 500 suppliers across 12 countries. Current payment terms are Net-60 (payment 60 days after invoice). Suppliers in developing countries struggle with cash flow while waiting for payment.

Tasks:

1. Design a programmable money solution where CBDC payment is automatically released when IoT sensors confirm delivery at the warehouse. Draw the flow diagram.
2. What oracle (external data source) is needed to trigger the smart contract? What happens if the oracle provides incorrect data?
3. Suppliers want immediate payment; the manufacturer wants to keep the 60-day float. Design a programmable escrow mechanism that satisfies both parties (hint: consider tokenized invoice discounting).
4. The manufacturer operates in the EU, where the digital euro will not be "programmable money." How can programmable *payments* (logic in the instruction, not the money) achieve the same result?
5. Identify two scenarios where automated payment execution could cause harm (e.g., goods are defective but payment already triggered).

Exercise 5: Self-Sovereign Identity for KYC

Scenario: A European bank currently spends €120M/year on KYC compliance. The average onboarding time is 14 days. 30% of applicants abandon onboarding due to document requirements. The bank processes 2 million KYC checks per year.

Tasks:

a) Design an SSI-based KYC flow. Identify: (i) who issues the verifiable credential, (ii) what claims it contains, (iii) how the bank verifies it, and (iv) what data the bank stores after verification.

b) The bank wants to verify "customer has annual income $>$ €50,000" without seeing the exact salary. Explain how zero-knowledge proofs enable this.

c) Estimate the cost savings if SSI reduces KYC processing time by 80% and abandonment by 50%. Assume each KYC check costs €60 currently and each abandoned customer represents €500 in lost lifetime revenue.

d) What happens if the issuer of the verifiable credential (e.g., the customer's previous bank) goes bankrupt? Design a credential revocation and re-issuance process.

Exercise 6: Cross-Border CBDC Interoperability

Scenario: Country A and Country B each have operational retail CBDCs running on different technology stacks. A citizen of Country A wants to pay a merchant in Country B using their CBDC wallet. Currently, this requires currency conversion through a correspondent banking chain (3–5 intermediaries, 2–3 day settlement, 3–5% fees).

Tasks:

a. Describe three architectural approaches to cross-border CBDC interoperability: (i) shared ledger, (ii) bridge protocol, (iii) hub-and-spoke via a neutral party (e.g., BIS).

b. For each approach, evaluate: latency, cost, privacy, and political acceptability.

c. The mBridge project (BIS Innovation Hub) connects multiple CBDCs for wholesale settlement. How does mBridge handle currency conversion? What is the role of the BIS in this architecture?

d. If Country A's CBDC is token-based and Country B's is account-based, what technical challenge arises at the conversion point?

Exercise 7: Unified Ledger Implementation

Scenario: A central bank decides to implement a prototype of the BIS unified ledger concept. The ledger will host: (i) wholesale CBDC, (ii) tokenized government bonds, and (iii) tokenized commercial bank deposits.

Tasks:

a) Design the atomic DvP (Delivery-vs-Payment) settlement for a tokenized bond purchase: what happens in a single transaction? List each step.

b) How does the unified ledger prevent a commercial bank from issuing tokenized deposits beyond its reserve ratio? What on-chain enforcement mechanism would you use?

c) A bond issuer defaults. How does the unified ledger handle default resolution for tokenized bonds? Is it different from traditional bond default?

d) Design the privacy layer: Bank A can see its own transactions but not Bank B's. How is this achieved on a shared ledger? (Consider zero-knowledge proofs, private channels, or confidential transactions.)

Exercise 8: End-to-End Convergence Case Study

Scenario: In 2030, a European investor wants to buy a tokenized corporate bond issued on the unified ledger, pay with digital euros, and authenticate using their EU Digital Identity Wallet.

Design the complete end-to-end flow:

a. **Identity:** The investor opens their eIDAS 2.0 wallet. What verifiable credentials are needed? (Hint: accredited investor status, KYC credential, tax residency.)

b. **Compliance:** The smart contract checks the investor's credentials against the bond's compliance rules (e.g., minimum investment, jurisdiction restrictions). Draw the verification flow.

c. **Settlement:** The investor transfers digital euros; the tokenized bond transfers to their wallet. Describe the atomic DvP transaction.

d. **Lifecycle:** The bond pays quarterly coupons. How are coupons distributed? What happens if the investor sells the bond mid-quarter?

e. **Failure modes:** Identify three things that could go wrong in this flow and propose mitigation for each.

Answer Key – Exercise 1

(1) Hybrid model recommended. Privacy expectations favor token-based for small transactions (cash-like anonymity), but AML regulations require account-based for large transactions. Threshold: transactions below €150 use token-based (offline-capable); above €150 require identity verification.
(2) Holding limit: €3,000–€5,000. Below €3,000: limited utility, citizens see no reason to adopt. Above €10,000: meaningful risk of deposit flight from commercial banks. A 98% banked population means most users have existing deposit relationships to protect.
(3) Offline payments: Yes, essential for rural areas and disaster resilience. Double-spend prevention in offline mode requires hardware-based security (secure element in the device) that enforces a maximum offline balance and transaction count. When reconnected, deferred settlement reconciles all offline transactions.
(4) Two-tier model: Central bank issues CBDC; commercial banks distribute via existing channels (apps, branches). Banks handle KYC, customer support, and wallet provision. This preserves the banking sector's role and leverages existing infrastructure.
(5) If the digital euro timeline is within 2–3 years: wait and align. If 5+ years: consider an interim national CBDC with migration path to digital euro. Launching an incompatible national CBDC risks costly integration later.

Answer Key – Exercise 2

(a) Comparison matrix:

Dimension	Custodial	Non-Custodial	MPC
Security	Provider risk	User risk	Distributed risk
UX	Best (app-like)	Worst (seed phrases)	Good (app + MPC)
Regulatory	Clear (licensed)	Ambiguous	Emerging
Recovery	Password reset	Seed phrase only	Threshold recovery
Cost	Medium	Low	High

(b) Custodial or MPC. For a 28-year-old with no crypto experience, seed phrase management (non-custodial) is a non-starter. MPC offers the best balance if budget allows; custodial is the pragmatic choice.
(c) MPC recovery: 2-of-3 threshold (user device, neobank server, backup cloud HSM). Phone loss: re-authenticate via neobank + cloud backup to reconstruct key. Neobank bankruptcy: user + cloud backup shares are sufficient to recover.
(d) MiCA requires custodial providers to hold a CASP license. If the neobank holds keys (custodial or MPC with key share), it must comply. Non-custodial wallets may fall outside MiCA scope but offer worse UX.

Answer Key – Exercise 3

(a) Total Year 1 cost: €2M (platform setup) + €400K (operations) + €800K (legal) = **€3.2M**.
(b) Additional annual rental income: €50M × 5.2% = **€2.6M/year**.
(c) Payback period: Year 1 net = €2.6M − €3.2M = −€600K. Year 2 ongoing cost = €400K; income = €2.6M; net = +€2.2M. Cumulative end of Year 2 = +€1.6M. **Payback within Year 2** (approximately 15 months from launch).
(d) Legal risks: (i) SPV legal challenge — if a court rules the SPV structure does not convey true ownership, token holders may lose their claim. Mitigation: robust legal opinion and jurisdiction selection. (ii) Cross-border enforceability — tokens sold globally but property law is local; jurisdictional conflicts possible. (iii) Regulatory reclassification — if tokens are reclassified as securities, the platform may need additional licenses. Mitigation: design tokens as securities from the start under MiFID II.

Answer Key – Exercise 4

(1) Flow: Manufacturer deposits CBDC into escrow smart contract → Supplier ships goods → IoT sensors at warehouse confirm receipt → Oracle transmits confirmation to smart contract → Smart contract releases CBDC to supplier's wallet.
(2) Oracle: IoT gateway aggregating sensor data (weight, GPS, timestamp). Risk: oracle manipulation (e.g., falsified delivery confirmation). Mitigation: multi-oracle consensus (require 2-of-3 independent confirmations) and dispute resolution window (24h delay before irrevocable release).
(3) Tokenized invoice discounting: Supplier tokenizes the invoice (claim on the escrowed CBDC). Supplier sells the tokenized invoice to a liquidity provider at a discount (e.g., 2%). Supplier receives immediate payment; manufacturer pays at day 60; liquidity provider earns the discount.
(4) Programmable payments via digital euro: The payment instruction (not the euro itself) contains the condition. A payment initiation service provider (PISP) monitors the IoT oracle and triggers an instant SEPA payment when conditions are met.
(5) Harm scenarios: (i) Defective goods: payment triggers on delivery confirmation, but goods fail quality inspection. Mitigation: add quality-check oracle or dispute window. (ii) Partial delivery: 80% of order arrives; smart contract designed for binary outcome pays 100%. Mitigation: proportional release logic.

Answer Key – Exercises 5–6

Exercise 5:
(a) Issuer: government registry or certified identity provider. Claims: full name, date of birth, nationality, address, tax ID, AML risk score. Verification: bank checks issuer's DID against trusted registry, verifies cryptographic signature on credential. Storage: bank stores a verification receipt (hash) but not the raw credential data.
(b) ZKP: The issuer's credential contains the exact salary. The holder uses a ZKP circuit to prove "salary $>$ €50,000" without revealing the value. The bank verifies the proof mathematically without learning the salary.
(c) Current cost: 2M $\times$ €60 = €120M. SSI cost: 2M $\times$ €12 (80% reduction) = €24M. Savings: €96M/year. Reduced abandonment: 2M $\times$ 0.30 = 600K abandons currently. 50% reduction = 300K saved $\times$ €500 = €150M recovered revenue. Total impact: **€246M/year**.
(d) Revocation: Credentials include a revocation registry check. If issuer goes bankrupt, a designated successor or regulatory body takes over the registry. Re-issuance: customer obtains a new credential from another trusted issuer using their DID.

Exercise 6 (key points):
(a) (i) Shared ledger: both CBDCs on one platform. (ii) Bridge: relay protocol translates between ledgers. (iii) Hub: BIS operates a conversion layer.
(b) Shared: fast, low cost, but politically difficult (shared sovereignty). Bridge: flexible, moderate speed, complex. Hub: trusted neutral party, moderate speed, most politically acceptable.
(d) Token-based $\rightarrow$ account-based conversion requires identity verification at the boundary. The token holder must authenticate to the account-based system.

Answer Key – Exercises 7–8

Exercise 7 (key points):
(a) Atomic DvP: (1) Buyer submits order + CBDC authorization; (2) Smart contract locks buyer's CBDC and seller's bond tokens; (3) Contract verifies both are valid and sufficient; (4) In a single atomic operation: CBDC transfers to seller, bond tokens transfer to buyer; (5) If either leg fails, both revert.
(b) On-chain reserve enforcement: smart contract queries the bank's CBDC reserve balance before allowing new deposit token issuance. If reserve ratio would fall below minimum, the issuance transaction reverts.
(d) Privacy: Use private data channels (like Hyperledger Fabric) or confidential transactions (like Zcash's shielded transactions). Each bank sees its own transactions in cleartext; other banks see only encrypted commitments.

Exercise 8 (key points):
(a) Credentials: eIDAS 2.0 identity, accredited investor VC, tax residency VC, KYC/AML VC from their bank.
(c) Atomic DvP: smart contract verifies credentials, locks digital euros and bond tokens, executes simultaneous swap.
(d) Coupons: smart contract reads token holder registry on payment date, distributes proportionally. Mid-quarter sale: accrued interest calculated by smart contract; buyer compensates seller for accrued coupon at time of trade.
(e) Failures: (i) Credential expired mid-transaction — mitigation: real-time validity check. (ii) Smart contract bug freezes funds — mitigation: audited contracts + emergency multisig. (iii) Digital euro system outage — mitigation: queued settlement with guaranteed execution.