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.