Quiz: Lesson 6.4 – Next-Generation Infrastructure

Module 6: The Infrastructure Problem

Prof. Dr. Joerg Osterrieder

(c) Joerg Osterrieder 2025–2026

Question 1 (Understand)

What is a Central Bank Digital Currency (CBDC)?

A. A private cryptocurrency issued by commercial banks

B. A stablecoin backed by central bank reserves

C. **A digital form of central bank money that is a liability of the central bank**

D. A blockchain-based token pegged to a fiat currency by a private company

(c) Joerg Osterrieder 2025–2026

Question 2 (Understand)

What is the key difference between a retail CBDC and a wholesale CBDC?

A. Retail CBDCs use blockchain; wholesale CBDCs use centralized databases

B. **Retail CBDCs are available to the general public; wholesale CBDCs are restricted to financial institutions for interbank settlement**

C. Retail CBDCs are token-based; wholesale CBDCs are always account-based

D. Wholesale CBDCs have higher transaction limits but are otherwise identical to retail CBDCs

Question 3 (Analyze)

In an account-based CBDC, transactions require identity verification. In a token-based CBDC, transactions require proof of possession (private key). What is the primary tradeoff?

A. Account-based is faster; token-based is slower

B. Token-based costs more to operate than account-based

C. **Account-based enables surveillance and AML enforcement but reduces privacy; token-based preserves privacy but makes AML compliance harder**

D. There is no meaningful tradeoff; both models are functionally equivalent

(c) Joerg Osterrieder 2025–2026

Question 4 (Apply)

The ECB proposes a digital euro holding limit of €3,000 per person. What is the primary policy reason for this cap?

A. To limit the total supply of digital euros in circulation

B. To prevent money laundering by capping individual holdings

C. **To prevent large-scale deposit flight from commercial banks to risk-free CBDC, which could destabilize bank funding**

D. To ensure that the digital euro is only used for small payments

Question 5 (Understand)

What distinguishes a custodial wallet from a non-custodial wallet?

A. Custodial wallets are only available on mobile devices
B. Non-custodial wallets do not support CBDC tokens
C. **In a custodial wallet the provider holds the private keys; in a non-custodial wallet the user holds the private keys**
D. Custodial wallets are always more secure than non-custodial wallets

(c) Joerg Osterrieder 2025–2026

Question 6 (Apply)

A cryptocurrency exchange suffers a hack and loses customer funds. Which wallet model were the affected customers most likely using?

A. Non-custodial hardware wallets

B. **Custodial wallets managed by the exchange**

C. MPC wallets with distributed key shares

D. Paper wallets stored offline

(c) Joerg Osterrieder 2025–2026

Question 7 (Understand)

What is Multi-Party Computation (MPC) in the context of digital wallets?

A. A consensus algorithm that validates transactions across multiple nodes

B. A technique for encrypting wallet addresses on the blockchain

C. **A cryptographic method where the private key is split into shares held by multiple parties, so no single party can sign a transaction alone**

D. A protocol for synchronizing wallet balances across multiple devices

(c) Joerg Osterrieder 2025–2026

Question 8 (Understand)

What does RWA tokenization mean?

A. Converting cryptocurrency into fiat currency through a regulated exchange

B. **Representing ownership rights to real-world assets (bonds, real estate, commodities) as digital tokens on a distributed ledger**

C. Creating a digital twin of a physical object using IoT sensors

D. Issuing a stablecoin backed by a basket of real-world assets

Question 9 (Analyze)

Traditional bond settlement takes T+1 (one business day). Tokenized bond settlement can be near-instant. Which of the following is the most significant financial benefit of faster settlement?

A. It eliminates the need for legal documentation

B. It removes counterparty credit risk entirely

C. **It reduces counterparty risk exposure and frees capital that would otherwise be locked during the settlement window**

D. It guarantees higher returns on the bond

(c) Joerg Osterrieder 2025–2026

Question 10 (Evaluate)

A government proposes using programmable CBDC to issue social welfare payments that can only be spent at approved retailers and expire after 90 days. Which concern is most critical?

A. The technical complexity of implementing expiry logic in smart contracts

B. The cost of deploying CBDC wallets to all welfare recipients

C. The risk of retailers refusing to accept CBDC payments

D. **The erosion of individual financial freedom and the precedent for government surveillance and control over personal spending**

Question 11 (Apply)

The Monetary Authority of Singapore (MAS) has proposed "purpose-bound money" (PBM). What does PBM do?

A. It binds CBDC to a specific blockchain protocol

B. It restricts CBDC usage to a single bank account

C. **It wraps CBDC units in a smart contract that imposes spending conditions, while the underlying CBDC remains fungible once unwrapped**

D. It permanently converts CBDC into a non-fungible token

Question 12 (Understand)

What is the difference between "programmable money" and "programmable payments"?

A. There is no difference; the terms are interchangeable

B. Programmable payments are faster than programmable money

C. **Programmable money has conditions embedded in the currency itself (e.g., expiry); programmable payments attach logic to the payment instruction while the money remains unconditional**

D. Programmable money requires blockchain; programmable payments do not

(c) Joerg Osterrieder 2025–2026

Question 13 (Understand)

What is a Decentralized Identifier (DID)?

A. A bank account number stored on a blockchain

B. A government-issued digital passport number

C. **A globally unique identifier controlled by the subject (not a central registry), enabling verifiable, self-sovereign identity**

D. A cryptocurrency wallet address

(c) Joerg Osterrieder 2025–2026

Question 14 (Apply)

Using SSI with verifiable credentials, an individual can prove they are over 18 without revealing their date of birth. What cryptographic technique enables this?

- A Symmetric key encryption
- B Public key infrastructure (PKI)
- C Digital signatures alone
- D **Zero-knowledge proofs (ZKPs)**

Question 15 (Analyze)

A large bank currently spends $200 million annually on KYC compliance across its global operations. How could SSI with verifiable credentials reduce this cost?

A. By eliminating the need for KYC entirely

B. By outsourcing KYC to the blockchain network

C. **By enabling customers to present pre-verified KYC credentials that the bank can verify cryptographically, eliminating redundant document collection and manual verification**

D. By using AI to automate document scanning (unrelated to SSI)

(c) Joerg Osterrieder 2025–2026

Question 16 (Analyze)

The BIS "unified ledger" concept proposes placing CBDCs, tokenized deposits, and tokenized assets on a single platform. What settlement innovation does this enable?

A. Faster batch processing at the end of each business day

B. Reduced transaction fees through economies of scale

C. **Atomic settlement (Delivery-vs-Payment), where asset and payment transfer occur simultaneously in a single transaction, eliminating settlement risk**

D. Automatic currency conversion between all CBDC jurisdictions

(c) Joerg Osterrieder 2025–2026

Question 17 (Apply)

An institutional investor purchases a tokenized bond using CBDC. The bond pays a 4% annual coupon. What happens to coupon payments in a fully tokenized environment?

A. The issuer manually transfers coupon payments to each bondholder's bank account

B. A custodian bank collects coupons and distributes them monthly

C. **A smart contract automatically distributes CBDC coupon payments to the wallet address holding the bond token on each payment date**

D. The bondholder must submit a claim form to receive each coupon payment

(c) Joerg Osterrieder 2025–2026

Question 18 (Evaluate)

China's e-CNY has been in pilot since 2020 with 260+ million wallets created, yet adoption for daily payments remains low. What is the most likely explanation?

A. The e-CNY technology is too slow for retail use

B. Chinese citizens do not trust digital payments

C. **Existing mobile payment solutions (Alipay, WeChat Pay) are already deeply embedded in daily life, and the e-CNY offers insufficient incremental value to change user behavior**

D. The Chinese government has not promoted the e-CNY sufficiently

Question 19 (Evaluate)

A central bank must choose between launching a CBDC on a permissioned blockchain or a centralized database. Which factor most strongly favors the centralized database?

A. Lower energy consumption

B. Better public perception of technological innovation

C. **Higher transaction throughput (100,000+ TPS) required for national retail payment volume, which current permissioned blockchains struggle to match**

D. Easier integration with existing cryptocurrency ecosystems

(c) Joerg Osterrieder 2025–2026

Question 20 (Evaluate)

Consider the convergence of CBDC, RWA tokenization, and SSI. Which of the following represents the greatest risk to this converged infrastructure?

A. Insufficient consumer demand for digital identity wallets

B. High electricity costs for running blockchain nodes

C. **Geopolitical fragmentation leading to incompatible national standards, preventing cross-border interoperability of CBDCs, tokens, and identity systems**

D. The expiry of current cryptographic standards due to quantum computing

(c) Joerg Osterrieder 2025–2026

Answer Key

1. (C) – Liability of the central bank
2. (B) – Public vs. financial institutions
3. (C) – Privacy vs. AML tradeoff
4. (C) – Prevent bank disintermediation
5. (C) – Who holds the private keys
6. (B) – Custodial wallet at the exchange
7. (C) – Key split across multiple parties
8. (B) – Real-world assets as tokens
9. (C) – Reduced risk and freed capital
10. (D) – Erosion of financial freedom
11. (C) – Smart contract wrapper on CBDC
12. (C) – Conditions in money vs. instruction
13. (C) – Subject-controlled identifier
14. (D) – Zero-knowledge proofs
15. (C) – Pre-verified credentials
16. (C) – Atomic DvP settlement
17. (C) – Smart contract auto-distribution
18. (C) – Existing solutions dominate
19. (C) – Throughput requirements
20. (C) – Geopolitical fragmentation

(c) Joerg Osterrieder 2025–2026