In-Class Assignment CB3: Privacy-Utility Frontier

Digital Finance – BSc Course | Prof. Dr. Joerg Osterrieder

Context. Three retail CBDC privacy designs compete: **(T)** Transparent – every transaction linked to real identity (China e-CNY pilot approach); **(P)** Pseudonymous – identity tokenised, central bank can de-anonymise with a court order (ECB's stated preference); **(Z)** Zero-knowledge – transactions revealed only via selective disclosure proofs (Project Tourbillon, SNB 2023). Evaluate each on four axes.

Q1. Fill in the **3×4 matrix** below. Use scores 1 (worst) – 5 (best) and note the key mechanism. Axes: (a) AML/sanctions enforcement, (b) citizen privacy, (c) programmability support, (d) infrastructure cost per transaction.

Solution. T (Transparent): AML = 5 (real-time monitoring), Privacy = 1 (full-graph visible to central bank + government), Programmability = 5 (any condition readable on-chain), Cost = 4 ($0.001/tx, similar to card rails). **P (Pseudonymous)**: AML = 3 (court-order latency of days blunts freeze-asset responses), Privacy = 3 (resistant to passive surveillance but state-breakable), Programmability = 4 (most conditions work on pseudonym; some – like means-testing – require identity reveal), Cost = 4 ($0.002/tx, similar to banks). **Z (Zero-knowledge)**: AML = 2 (only selective disclosure; sanctions enforcement relies on wallet whitelists), Privacy = 5 (mathematically guaranteed, even against state), Programmability = 2 (only predicates the user consents to reveal), Cost = 1 ($0.05–0.20/tx in 2026, ZK-proof generation is compute-heavy). Rule of thumb: privacy and AML are exact opposites; Z is 50× more expensive.

Q2. For each of 3 use cases, recommend the best design. One line each: (i) a €200 grocery purchase, (ii) a €5M wholesale DvP, (iii) a whistleblower receiving €50k from a foreign NGO.

Solution. (i) **Z (or cash)**: €200 groceries carries no AML interest; citizens deserve privacy equal to cash – T would chill speech (e.g. abortion clinic co-pays, minority-press subscriptions). (ii) **T or P**: institutional counterparties are not "citizens" in the civil-liberties sense and need full AML/audit trails. Z adds cost and complexity without clear benefit when both parties are KYC'd banks. (iii) **Z with constitutional carve-out**: whistleblower protection requires mathematical privacy, not promises – a court order in an authoritarian jurisdiction would reveal P. The design should allow receiving anonymous flows above KYC thresholds only into verified journalist/NGO wallets with a statutory safe-harbour.

Q3. The ECB's current proposal is **"tiered privacy"**: tx $< e100$ = Z-like, €100–1,000 = P with KYC, $> e1{,}000$ = T with enhanced monitoring. Identify **one structural flaw** in this design. One sentence.

Solution. Structural flaw: smurfing resistance – a €10k payment can be split into 120 sequential €83 payments between the same two wallets, each qualifying as Z, defeating the AML intent at the top tier without any new technology. Real-world precedent: crypto mixers (Tornado Cash) functioned as legal services until 2022 because each individual tx was below the AML threshold while aggregate flows laundered $7B. Acceptable alternatives: (i) *wallet-level* not *tx-level* tiering (KYC below the threshold too), (ii) velocity checks inside Z zone (max 3 tx/minute), (iii) mandatory 24h aggregate visibility to the central bank even if individual-tx privacy is preserved.