In-Class Assignment TP1: The Anonymous Transaction

Digital Finance – BSc Course Prof. Dr. Joerg Osterrieder

Context. Alice in Berlin owes Bob in Manila $10,000 for a used camera. They have never met, do not share a bank, and want to settle today. Design a protocol that does *not* rely on any bank, card network, or state-backed intermediary. You may assume both parties own a laptop and an internet connection.

Q1. List **3 trust assumptions** a traditional bank transfer would require here (the things Alice must implicitly trust the bank + network to do correctly).

Solution. (i) **Solvency**: the bank holds enough reserves to honour Alice's withdrawal on demand; (ii) **Honest bookkeeping**: the bank's ledger debits Alice and credits Bob's bank truthfully, with no double-spend or silent reversal; (iii) **Correspondent-chain cooperation**: every bank in the 3–5-hop SWIFT route (Berlin → USD correspondent → Manila) processes, converts, and forwards without freezing. Acceptable substitutes: KYC accuracy, sanctions-screening, FX fairness, service availability.

Q2. Your protocol uses a public blockchain with a USD-pegged stablecoin (e.g. USDC on Ethereum). Walk through the 4 technical steps Alice executes, *and* identify the **3 new trust assumptions** she has introduced.

Solution. Steps: (1) Alice buys 10,000 USDC on a regulated ramp, (2) transfers to her self-custody wallet, (3) pays gas and sends to Bob's wallet address, (4) Bob off-ramps to peso or holds. New trust: (i) **Stablecoin issuer solvency** (Circle really holds $10k in T-bills 1:1), (ii) **Smart-contract correctness** (USDC contract has no blacklist exploit, no admin mint), (iii) **Chain liveness + finality** (Ethereum validators process her tx and do not reorg). Bonus: trust that Bob's off-ramp passes Philippines BSP sanctions screening.

Q3. Name *one* failure mode where the blockchain protocol is *worse* than the bank, and one where it is *better*. One sentence each.

Solution. **Worse**: lost private key = permanent 100% loss, no recourse; the bank would re-issue a card. **Better**: no correspondent bank can freeze Alice's transfer mid-route for a sanctions false-positive (a $10k remittance to the Philippines is frozen 3–8% of the time on USD rails). Other "better" answers: 24/7 settlement, fixed-cost fee ($1–5 vs $30–60 on SWIFT), censorship-resistance. Other "worse" answers: volatile gas costs, irreversible fraud, tax/regulatory ambiguity in recipient country.