In-Class Assignment TP3: Escrow vs. Smart Contract

Digital Finance – BSc Course Prof. Dr. Joerg Osterrieder

Context. Alice (buyer) wants to pay Bob (seller) $2,500 for 1 ETH. Design A: traditional lawyer-escrow (e.g. Escrow.com); lawyer holds fiat until delivery confirmed. Design B: on-chain escrow smart contract; Alice deposits $2,500 stablecoin, Bob deposits 1 ETH, release conditions coded. Assume honest, technically competent parties in both cases.

Q1. List the **5 steps** for each design in chronological order. Where does each design place the "trust pivot" (the single point whose failure breaks the deal)?

Solution. A (lawyer-escrow): (1) Alice wires $2,500 to escrow account; (2) Bob ships ETH keys to escrow agent; (3) agent verifies receipt; (4) agent releases $2,500 to Bob and keys to Alice; (5) escrow fee of 1–3% deducted. **Trust pivot: the lawyer/escrow company** (solvency + honesty). **B (smart contract)**: (1) Alice and Bob agree on contract address; (2) Alice deposits $2,500 USDC; (3) Bob deposits 1 ETH; (4) either confirms delivery and releases (or a dispute triggers oracle arbitration); (5) gas $\approx$ $5–20. **Trust pivot: the smart contract's source code** (plus the oracle, if arbitration is used).

Q2. Give **2 failure modes** for each design.

Solution. A failures: (i) escrow firm insolvency (Escrow.com competitor $2.2M default 2019); (ii) corrupt agent collusion with Bob (agent releases funds while Bob never ships). Acceptable alternatives: regulatory freeze, social-engineering phishing, jurisdictional refusal to enforce. **B failures**: (i) smart-contract bug (e.g. a re-entrancy attack drains escrow — DAO 2016, Parity 2017); (ii) key loss (Alice loses private key = $2,500 gone forever); bonus — oracle manipulation during dispute arbitration (Mango Markets 2022).

Q3. Which design would *you* pick for (a) a one-off $2,500 P2P trade between strangers, (b) a $25M institutional OTC settlement? Justify in one line each.

Solution. (a) **Smart contract**: $5–20 gas beats a 1–3% escrow fee ($25–75), and the contract is auditable by both parties ex ante. Only viable if both parties own wallets. (b) **Lawyer-escrow** (or a hybrid "legal wrapper" such as ISDA + on-chain settlement): $25M needs enforceable recourse — a smart-contract bug means $25M gone, while a lawyer has professional indemnity insurance (typically 5–10% of AUM) and a regulator of last resort. Acceptable alternative: institutional-grade DvP platforms (Fnality, Onyx) that legally wrap smart contracts.