Prof. Dr. Joerg Osterrieder

Content Reference: The Trust Problem

Digital Finance – BSc Course – Standalone Lecture

Learning Objectives

After engaging with this reference sheet and the companion lecture, you will be able to:

- **Explain** why trust is the binding constraint on exchange between strangers [Understand]
- **Compare** centralised, hybrid, and decentralised trust architectures [Analyze]
- **Apply** the double-spend and Byzantine-generals framings to candidate systems [Apply]
- **Evaluate** which financial services are credibly disintermediatable [Evaluate]

1. Key Definitions

- **Trust gap** — the cost, delay, or outright refusal that arises when two strangers who would both benefit from exchange cannot verify each other.
- **Double-spend problem** — digital money is data, and data is trivially copyable; without a shared ledger, Alice can pay Bob and Carol with the same coin.
- **Byzantine fault tolerance (BFT)** — a system's ability to agree on state when some participants are malicious or unreachable, not just crashed.
- **Centralised trust** — a single authority (a bank, registry, notary) certifies state; cheap to build, but single point of failure.
- **Federated trust** — a small set of known institutions jointly certify state (SWIFT, VisaNet, the ACH network); intermediate cost, shared veto.
- **Decentralised trust** — no privileged actor; state is produced by an open protocol and the economic incentives of many pseudonymous validators.
- **Trustless system** — a slight misnomer: participants still trust the protocol, the cryptography, and the economic incentives – they simply do not need to trust named counterparties.
- **Disintermediation** — direct exchange between two parties that previously required a bank, broker, registrar, or notary to sit in between.

2. Core Concepts

The trust stack: what banks and courts actually sell

Modern finance is a stack of *trust services*: identity verification, settlement finality, dispute adjudication, and record-keeping. Each layer costs money (fees, spreads, float) and time (T+2, week-long onboarding, multi-year lawsuits). Cryptography and decentralised consensus replicate some of these layers in software – but not all of them.

What code can replace: transaction finality, record-keeping, programmable settlement, non-custodial exchange.
What code cannot replace: off-chain identity, real-world dispute resolution, insurance against protocol bugs, adaptive regulation.
The honest framing is *trust* ***re-allocation***, not trust abolition: risk moves from named counterparties to anonymous protocol assumptions.

3. Key Figures & Data

- **1.4 billion** adults globally are unbanked (World Bank Findex 2024). The binding barrier cited most often is documentation and verifiable identity – a trust problem, not a wealth problem.

- **SWIFT** connects ~11,000 banks across 200+ countries and clears roughly 45 million messages per day; it is a federated-trust system, not a payment rail.
- **Bitcoin** has settled over $100 trillion cumulative value (2009–2025) without a central operator and with zero protocol-level double-spend events.
- **The DAO** (2016) lost ~$50M in ether to a re-entrancy bug; the community's response was to hard-fork Ethereum, demonstrating that decentralised systems still fall back on off-chain social trust when things break.
- **Remittance cost** averages 6.2% globally (World Bank Q4 2024); correspondent-bank trust chains are the primary cost driver, not FX.

4. Worked Example

Pricing the trust layer in a cross-border transfer

Scenario. Amina in Nairobi sends $200 to her brother Tariq in Manila.

Correspondent-bank path (trust chain of 4 named banks):

Sender bank FX spread	$6.00 (3%)
SWIFT + wire fee	$25.00
Correspondent fee (US)	$15.00
Receiving bank fee	$8.00
Total cost	**$54.00** (27% of principal)
Settlement time	2–5 business days

Stablecoin path (trust in USDC issuer + Ethereum protocol):

On-ramp fee (bank → USDC)	$2.00 (1%)
On-chain transfer	$0.50 (L2 gas)
Off-ramp fee (USDC → PHP)	$2.00 (1%)
Total cost	**$4.50** (2.25% of principal)
Settlement time	2–10 minutes

The $49.50 saved is a direct measurement of what the correspondent trust chain charges for its service. The stablecoin path is not trust-free – Amina and Tariq now trust Circle (the USDC issuer), Ethereum's validators, and the two on-/off-ramp providers – but the trust chain is shorter and priced competitively.

5. Self-Check Questions

1. State, in one sentence each, what a *double-spend* attack is and why a centralised bank does not have to worry about it.
2. Give one real-world financial service that *cannot* plausibly be moved to a decentralised system and explain why.
3. A colleague claims "blockchain removes the need for trust." Correct the claim in one sentence using the term *trust re-allocation*.

[Answers hidden in student version. Compile instructor PDF with `\AtBeginDocument{\solutionstrue}` *prepended to the input invocation.]*

6. Further Reading

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* The canonical articulation of the double-spend problem without a trusted third party.
- Lamport, L., Shostak, R. & Pease, M. (1982). "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems*, 4(3), 382–401.
- Catalini, C. & Gans, J. (2020). "Some Simple Economics of the Blockchain." *Communications of the ACM*, 63(7), 80–90.
- World Bank Global Findex Database 2024. worldbank.org/globalfindex.

- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press. Chapter 3 ("The Double-Spend Problem") is the best textbook treatment.
