# In-Class Activity: TBM3 — Model Matching — SOLUTIONS

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

Trustless Business Models | 15–18 min | Individual → Pair-share

---

**Context:** Six models: (1) DeFi Lending, (2) Tokenized Assets (RWA), (3) DAOs, (4) Supply Chain Provenance, (5) SSI, (6) Programmable Money. Coase costs: *search / bargaining / enforcement.*

**Exercise 1 (completed):**

| # | Scenario | Best model | Cost |
|---|---|---|---|
| A | Kenyan coffee cooperative: fair-trade origin for EU buyers without a paper certifier. | **(4) Supply Chain Provenance** | **E** (enforcement) |
| B | Swiss asset manager fractionalising a CHF 15 M Picasso for 300 global accredited investors. | **(2) Tokenized Assets** | **S** (search) |
| C | Remittance app auto-releasing funds when a GitHub PR is merged. | **(6) Programmable Money** | **E** (enforcement) |
| D | DeFi user borrowing $15,000 against $40,000 ETH without selling, for 6 months. | **(1) DeFi Lending** | **B** (bargaining) |
| E | $120 M treasury: community — not a foundation — decides quarterly grants. | **(3) DAOs** | **B** (bargaining) |
| F | Patient sharing medical records with a foreign specialist without handing over credentials. | **(5) SSI** | **S** (search) |

**Exercise 2 (sample justifications):**

**Row A (model 4, cost E — enforcement):** The coffee cooperative already has the beans and the buyers exist — search and bargaining are handled. What fails in practice is *enforcing* that the beans sold under a "fair-trade" label actually came from the cooperative. An immutable on-chain provenance trail makes that claim auditable without a trusted certifier. Why not the others? (1) (2) (6) don't address certification; (3) is overkill for 1 co-op; (5) is for personal identity, not goods.

**Row D (model 1, cost B — bargaining):** The user *knows* they want a loan and *knows* which protocol offers it — search cost is near zero. The hard part is negotiating terms with a stranger who can't credit-check them cheaply. Overcollateralization algorithmises the bargain: the protocol "offers" uniform terms to everyone; take it or leave it. Why not the others? (2) (4) (5) (6) don't issue credit; (3) is a governance primitive, not a credit primitive.

**Exercise 3 (residual risks):**

**A:** You still trust *whoever scans the QR on the bean sack at origin* — the "oracle problem". On-chain records can't detect off-chain fraud at the point of first data entry.

**B:** You still trust *the legal entity holding the Picasso in custody.* A token is a claim on the painting, not the painting itself; if the vault empties or the contract is repudiated, the token is worthless. Also trust the regulator allowing the fractional-share structure.

**D:** You still trust *the smart contract code, the price oracle, and the chain's liveness.* Oracle manipulation has caused multiple nine-figure DeFi exploits (e.g., Mango Markets Oct 2022, $114 M).

**Debrief:** Most real-world pipelines combine *two or three* models — e.g., a tokenized real-estate platform needs (2) Tokenized Assets for the fractional shares, (5) SSI for KYC, and (6) Programmable Money for rent distribution. "One model fits all" is the exception, not the rule.

---

**Answer Key** **E1:** A → 4/E, B → 2/S, C → 6/E, D → 1/B, E → 3/B, F → 5/S. **E2:** A: enforcement drops (audit replaces certifier). D: bargaining drops (algorithmic overcollateralization replaces credit negotiation). **E3:** A: oracle / first-data-entry trust. B: custodian + legal wrapper. D: oracle + smart-contract + chain liveness. Core lesson: trustless ≠ risk-free — every model **relocates** trust; know where it moved to.