Pre-Class Discovery: Supply Chain Transparency — SOLUTIONS

Digital Finance – BSc Course Prof. Dr. Joerg Osterrieder

Complete before class. No prior knowledge required. Work alone or in pairs.

Activity 1: Trace Your Lunch

Pick one item from your last meal (e.g. a banana, a chicken sandwich, a coffee).

(a) Trace it back 3 steps from your plate. Fill in the table:

Step	Actor	What you do NOT know
3 (you)	Retailer / canteen	
2	Distributor	
1	Producer / farmer	

(b) What information would you *need* to verify the item is organic, fair-trade, or sustainably sourced?

Activity 2: The Trust Gap

A blockchain records that your coffee is certified organic. But the blockchain only stores what someone typed in. The coffee itself never touches the chain.

(a) This is called the "oracle problem." In one sentence, explain why a blockchain cannot verify physical-world facts by itself.

(b) List 3 approaches to bridge the gap between the physical bean and the digital record.
Hint: think about IoT sensors, third-party audits, and economic incentives.

(c) For each approach, name one weakness or way it could be defeated.

Activity 3: EU Digital Product Passport Impact

Starting in 2027, the EU requires Digital Product Passports (DPPs) for textiles, batteries, and electronics—a full lifecycle record on-chain or in a verified database.

Consider a $5 t-shirt sold by a fast-fashion brand:

(a) Estimate the implementation cost per unit to create a DPP (think: scanning, data entry, storage, QR code, IT systems).

(b) Who ultimately pays this cost? The brand, the factory, or the consumer?

(c) Does the DPP requirement help or hurt small producers in developing countries? Give one argument for each side.

Answer Key

A1: (a) Typical unknowns: retailer—markup, storage conditions; distributor—transport temperature, delays, mixing of batches; producer—pesticide use, labour conditions, exact origin plot. (b) Certifications, lab test results, GPS coordinates of farm, audit trail of every handler, temperature logs.

A2: (a) A blockchain validates transaction rules (signatures, balances) but cannot sense the physical world; it relies on external inputs (oracles) that can lie. (b) IoT sensors (e.g. temperature/GPS tags on shipments), independent third-party audits at checkpoints, stake-and-slash incentives (participants post a bond that is forfeited if fraud is detected). (c) IoT: sensors can be tampered with or relocated. Audits: auditors can be bribed or fooled. Incentives: fraud profitable if gains exceed the bond.

A3: (a) Estimates range from \$0.05–\$0.50 per unit (scanning + data entry + IT amortised over volume). (b) Initially the brand pays for IT; long-run, the cost is passed to consumers via higher prices or absorbed by squeezing factory margins. (c) Helps: levels the playing field—transparent producers gain market access. Hurts: compliance cost is proportionally higher for small producers who lack IT infrastructure.