Supply Chain Provenance: Trust What You Buy

Module 3: The Trust Problem — Standalone Lecture

Prof. Dr. Joerg Osterrieder

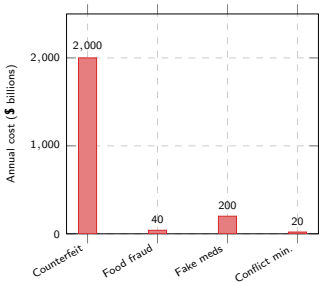
Digital Finance — BSc Course

Standalone lecture — explores how blockchain and IoT attempt to solve the $4.2 trillion counterfeiting problem.

Why can you not trust that what you buy is what it claims to be?

The scale of the problem:

- Global trade in counterfeit goods: ∼$464B in 2021, about 2.5% of world trade (Source: OECD/EUIPO, "Global Trade in Fakes", 2024)
- Food fraud: affects 10% of commercially sold food products
- Counterfeit medicines: 1 in 10 medical products in developing countries is falsified (WHO)
- Conflict minerals: fund armed groups in Central Africa



Estimates vary across sources (OECD/EUIPO 2024; WHO; various regulators). The true scale is unknown because successful counterfeiting goes undetected.

Why existing systems fail:

- **Paper certificates:** easily forged, lost, or altered
- **Centralised databases:** controlled by one party, can be edited
- **Complex supply chains:** 8–12 handoffs from source to consumer
- **No interoperability:** each company uses its own tracking system
- **Audit gaps:** inspections happen annually, fraud happens daily

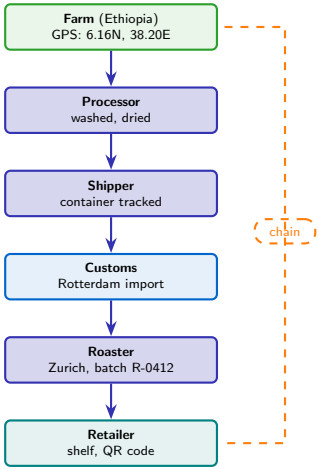
Key insight: The longer the supply chain, the more opportunities for fraud — and the harder it is to verify authenticity.

Counterfeiting thrives because supply chains are opaque — each handoff is an opportunity to substitute, dilute, or mislabel products.

Imagine scanning your coffee bag and seeing the exact farm where it was grown

The experience:
You buy a bag of coffee at the supermarket. You scan the QR code on the packaging with your phone. Instantly you see:

- **Farm:** Yirgacheffe cooperative, Ethiopia (GPS coordinates)
- **Harvested:** March 2026, Lot #4472
- **Certification:** Fair-trade verified, organic certified
- **Processing:** Washed, dried 14 days at station #7
- **Shipped:** Container MSKU-4829371, Port of Djibouti to Rotterdam
- **Arrived:** April 2, 2026, customs cleared Hamburg
- **Roasted:** April 8, Zurich roastery, batch R-2026-0412
- **Temperature:** never exceeded 25C during transit (IoT = Internet of Things: physical sensors that automatically record temperature, location, humidity, etc.)



Today's reality:
The label says "100% Ethiopian Arabica" — but you have no way to verify it. The paper trail stops at the importer.

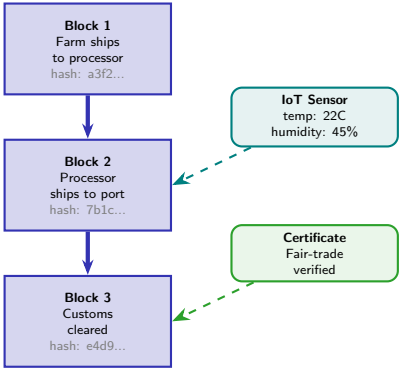
The promise: Every handoff recorded, every claim verifiable, every certificate unforgeable.

Blockchain supply chain tracking turns "trust the label" into "verify the journey" — every handoff becomes an immutable record.

How does blockchain create an unforgeable audit trail from source to shelf?

Definition: Supply Chain Provenance

A system that records every handoff in a product's journey as an immutable blockchain transaction, creating a verifiable audit trail from raw material to final consumer.



How it works:

1. Each participant (farm, processor, shipper, retailer) has a blockchain identity
2. At every handoff, the sender and receiver record a transaction
3. IoT sensors add data automatically (temperature, humidity, GPS)
4. Certifications are attached as verifiable credentials
5. The consumer scans a QR code to see the full history

Why blockchain and not a normal database?

- **Immutability:** no participant can alter past records
- **Shared access:** all parties see the same data
- **No single owner:** the database is not controlled by one company
- **Timestamped:** every entry has a cryptographic timestamp

Each block in the chain records one handoff — together they create an unforgeable history that no single participant can alter after the fact.

How does De Beers track 30% of global diamond production from mine to store?

De Beers Tracr platform:

- Launched 2022, tracks diamonds mine-to-retail
- Covers 30% of global diamond production by value
- Records each diamond's unique characteristics (carat, cut, clarity, colour)
- Creates a "digital twin" on blockchain at the mine
- Every handoff (cutter, polisher, dealer, retailer) adds a record

The problem it solves — conflict diamonds:

- Kimberley Process (2003) relies on paper certificates
- Paper certificates are easily forged or reused
- Conflict diamonds fund armed groups in Africa
- Consumers cannot verify origin at the jeweller

How Tracr prevents laundering:

- Each diamond registered at source with unique ID
- Ownership changes recorded immutably
- Unregistered diamonds cannot enter the tracked supply chain
- Retailers can prove provenance to consumers

Metric	Tracr
Launched	2022
Coverage	30% of global production
Diamonds tracked	Millions
Participants	Miners, cutters, dealers, retailers
Technology	Private blockchain
Data per diamond	ID, 4Cs, provenance, owner history
Consumer access	QR code at retail

Limitation: Tracr only tracks diamonds that enter the system at a participating mine. Diamonds from non-participating sources remain untraceable.

Key insight: Blockchain provenance is only as good as the initial data entry. If a conflict diamond is registered as legitimate at the mine, the blockchain will faithfully record a lie.

De Beers Tracr shows blockchain provenance at scale — but it works because De Beers controls the mines where data entry begins.

Worked example: tracking a coffee bean through 8 handoffs from farm to cup

The journey of Lot #4472:

1. Farm (Ethiopia): Farmer registers harvest. GPS, weight (500 kg), variety (Arabica), date.

2. Cooperative: Aggregates lots from 12 farmers. Quality grading. Fair-trade certification attached.

3. Dry mill: Hulled, sorted, graded. Weight: 420 kg (moisture loss). IoT: humidity 11%.

4. Export warehouse: Bagged, container MSKU-4829371. Export licence attached.

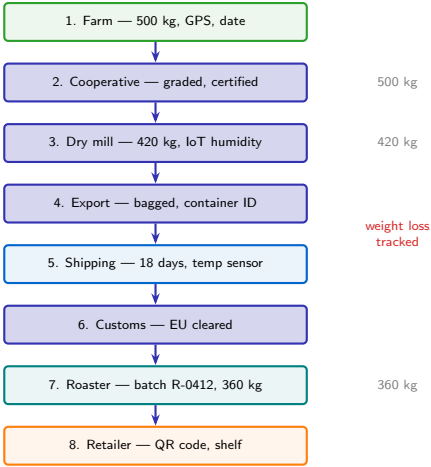
5. Shipping: Djibouti to Rotterdam. Temperature sensor: max 24C. Transit: 18 days.

6. Import customs: EU phytosanitary check. Cleared April 2.

7. Roaster (Zurich): Roasted April 8. Batch R-2026-0412. Weight: 360 kg (roast loss).

8. Retailer: Packaged, QR code printed. Consumer scans to see full history.

Key insight: 8 handoffs, 8 blockchain transactions, one unbroken chain of custody.



Weight decreases from 500 kg to 360 kg through processing — blockchain tracks this shrinkage, making it harder to substitute cheaper beans mid-chain.

Blockchain records are immutable — but who guarantees the data entered is true?

The physical-digital gap (the oracle problem):

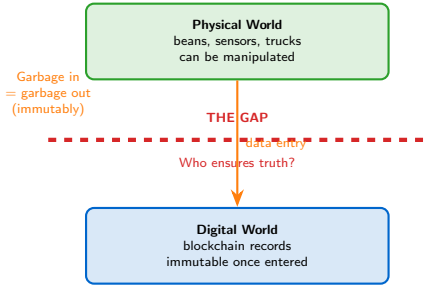
- Blockchain guarantees that records cannot be changed after entry
- But it *cannot* guarantee that the data entered is correct
- If a farmer registers conventional beans as organic, the blockchain will faithfully record a lie

Specific attack vectors:

- **False initial entry:** mislabelling origin, grade, or certification
- **IoT sensor tampering:** physically moving sensors to fake locations
- **Collusion:** two parties agree to skip a handoff and fake the record
- **Physical substitution:** swap goods after the blockchain scan

Cost barriers:

- IoT sensors cost $5–50 per unit
- Blockchain transaction fees add up across millions of products
- Small-scale producers in developing countries cannot afford the tech
- The people who most need provenance are least able to pay for it



Warning: Blockchain does not verify truth. It only ensures that *whatever is entered* cannot be changed later. An immutable lie is still a lie.

The physical-digital gap is the fundamental limitation of all blockchain provenance systems — immutability does not equal truthfulness.

Where is blockchain supply chain tracking deployed today — and what is coming?

Major deployments (as of 2026):

- **IBM Food Trust:** Walmart (leafy greens), Nestlé, Carrefour — *platform wound down in 2024; participants migrating to private alternatives*, a cautionary tale on consortium fragility
- **VeChain:** luxury goods authentication, wine provenance
- **LVMH Aura:** Louis Vuitton, Cartier, Prada, now ∼30 houses — luxury consortium
- **De Beers Tracr:** diamond mine-to-store tracking (30% of natural diamonds)
- **Everledger:** wine, diamonds, art provenance

Platform	Sector	Scale
IBM Food Trust	Food	Wound down 2024
VeChain	Luxury	100+ brands
LVMH Aura	Luxury	30 houses
De Beers Tracr	Diamonds	30% global
Everledger	Multi	2M+ items

EU Digital Product Passport timeline:

EU Digital Product Passport (DPP):

- **Mandate:** EU regulation requiring digital passports for products
- **Timeline:** phased rollout starting 2027 (batteries first)
- **Scope:** textiles, electronics, construction materials
- **Data:** origin, materials, carbon footprint, recyclability
- **Technology:** blockchain is one possible backend

Key insight: Regulation is forcing supply chain transparency — the EU DPP will make provenance tracking mandatory, not optional.

The EU Digital Product Passport will make supply chain transparency a legal requirement for hundreds of product categories by 2030.

Who wins and who loses when supply chains become transparent?

Winners:

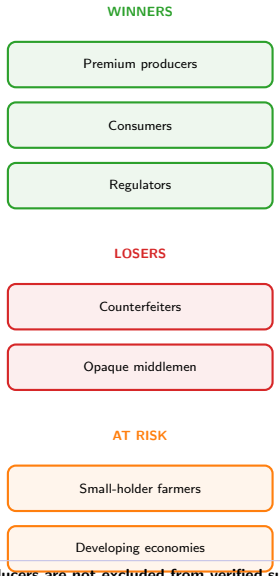
- **Premium producers:** can prove origin and quality, charge premium
- **Consumers:** can verify claims (organic, fair-trade, conflict-free)
- **Regulators:** real-time audit trails replace periodic inspections
- **Brands:** protect reputation by proving authenticity

Losers:

- **Counterfeiters:** harder to fake provenance (but not impossible)
- **Middlemen:** transparent pricing reduces margin for intermediaries

The small-holder challenge:

- 500 million smallholder farms produce 80% of food in developing countries
- Most lack smartphones, internet, or the $5–50 per sensor cost
- If they cannot participate, provenance tracking excludes the most vulnerable producers
- Risk: blockchain supply chains benefit large corporations, not small farmers



Key insight: Supply chain transparency is valuable — but the cost of participation risks creating a two-tier system.

Blockchain provenance helps those who can afford to participate — the challenge is ensuring small producers are not excluded from verified supply chains

So what? One sentence to remember about blockchain supply chains

Blockchain makes records immutable —

but it cannot guarantee that the data entered

at the first step is truthful.

What blockchain solves	What blockchain does not solve	What helps close the gap
Tamper-proof records	Initial data accuracy	IoT sensors
Shared visibility	Physical-digital gap	Satellite verification
Automated audit trails	Cost for small producers	AI anomaly detection
Timestamped custody chain	Collusion between parties	Regulatory mandates (EU DPP)

Blockchain provenance is a necessary but not sufficient condition for supply chain trust — immutability plus truthful data entry together create verifiable chains.

Your turn: will the EU Digital Product Passport reduce counterfeiting or just add cost?

Discussion Question

The EU mandates Digital Product Passports for batteries (2027), textiles (2028), and all products (2030). Every product must have a scannable record of its origin, materials, and environmental footprint.

Debate: *Will the EU Digital Product Passport reduce counterfeiting and improve sustainability — or will it primarily add compliance cost and burden small producers?*

- Who pays for the infrastructure — producers, consumers, or taxpayers?
- Can small-holder farmers in developing countries participate?
- What happens to products from countries that do not adopt the standard?
- Does transparency alone change consumer behaviour?

Further Reading

- EU Digital Product Passport regulation: `ec.europa.eu/environment/ecodesign`
- Kshetri (2018), "Blockchain's roles in meeting key supply chain management objectives"
- Casey & Wong (2017), "Global Supply Chains Are About to Get Better, Thanks to Blockchain," *Harvard Business Review*

When Labels Lie

Provenance tells you where the label was made, not the product.

Provenance systems track where labels were created — but who checks whether the label matches reality?

Learning Objectives

After completing this lecture, you will be able to:

1. **Quantify** the scale of supply chain fraud across food, pharmaceuticals, and minerals [Understand]
2. **Trace** a product through a blockchain-based provenance system, identifying each handoff as a transaction [Apply]
3. **Explain** how IoT sensors bridge the physical-digital gap and where they fail [Analyze]
4. **Evaluate** the "garbage in, garbage out" limitation of on-chain provenance [Evaluate]
5. **Assess** the cost barriers that exclude 500 million smallholder farmers from provenance systems [Evaluate]

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

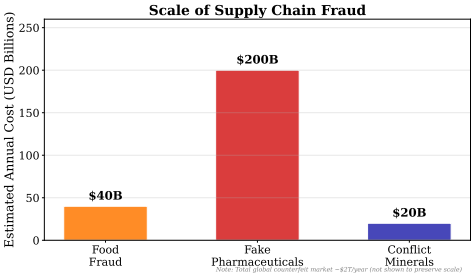
Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.

The $4.2 Trillion Counterfeiting Problem

Global counterfeiting costs $4.2 trillion per year (OECD, 2023):

- **Fake pharmaceuticals:** $200B — 1 million deaths/year (WHO)
- **Food fraud:** $40B — adulteration, mislabelling, origin fraud
- **Conflict minerals:** $20B — funding armed groups in DRC
- Counterfeit luxury goods, auto parts, electronics make up the rest

Core issue: You cannot verify what you cannot trace.



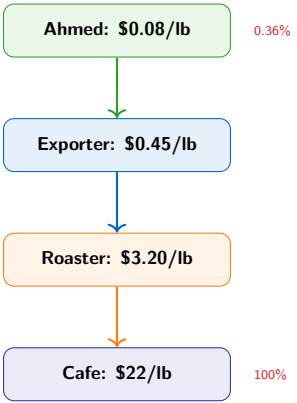
What you see: three bars showing food fraud ($40B), fake pharma ($200B), and conflict minerals ($20B). Total counterfeit market is $2T+.

Meet Ahmed — Coffee Farmer, Sidamo Region, Ethiopia

Ahmed's situation:

- Grows **single-origin Arabica** on 0.5 hectares
- Earns **$0.08 per pound** at the farm gate
- The same beans sell for **$22 per pound** at a Zurich specialty cafe
- **275× markup** — Ahmed captures 0.36% of retail value

The trust problem:
Ahmed has no way to prove his beans are genuinely single-origin. Exporters routinely mix origins. Roasters cannot verify claims.
Question: Who benefits from this opacity?



Ahmed represents 25 million coffee farming families worldwide. Most earn below $2/day despite producing a $460B global industry.

Meet Grace — Mother, Lagos, Nigeria

Grace's situation:

- Her 4-year-old son has malaria — needs artemisinin-based treatment
- She buys medicine from a local pharmacy for 2,500 Naira ($3.10)
- **The pills contain no active ingredient** — they are counterfeits
- Her son's condition worsens. She has no way to verify the medicine

WHO Estimate

500,000+ deaths/year from fake medicines

Malaria + pneumonia are most affected

The scale of fake pharmaceuticals:

- **10.5%** of medicines in low/middle-income countries are substandard or falsified (WHO, 2023)
- **1 in 10** medical products fails quality testing
- Sub-Saharan Africa: up to **30%** of antimalarials are fake

This is not a supply chain problem. It is a life-or-death problem.

Nigeria's NAFDAC introduced a scratch-and-verify SMS system (mPedigree) in 2009 — an early non-blockchain provenance solution.

Meet Marco — Olive Oil Producer, Puglia, Italy

Marco's situation:

- Third-generation producer of **extra virgin olive oil (EVOO)**
- Costs €8/litre to produce authentic Puglia EVOO
- Competitors sell "Italian EVOO" for €3/litre — blended with cheaper oils or chemically deodorised lampante oil
- Marco **cannot compete on price** against fraud

The olive oil fraud problem:

- **70%** of imported EVOO in the US fails quality tests (UC Davis, 2011)
- Italian authorities seized 2,000+ tonnes of fraudulent oil in 2022
- "Made in Italy" labels applied to non-Italian oils at bottling

Trust destruction: Fraud by competitors undermines Marco's brand.

Price Gap

Authentic: €8/L
Fraudulent: €3/L

Honest producers priced out

The "Italian olive oil problem" mirrors wine fraud, honey adulteration, and Manuka honey counterfeiting — all origin-dependent premium products.

Do you trust the “organic” label on your food?

A: Yes, fully

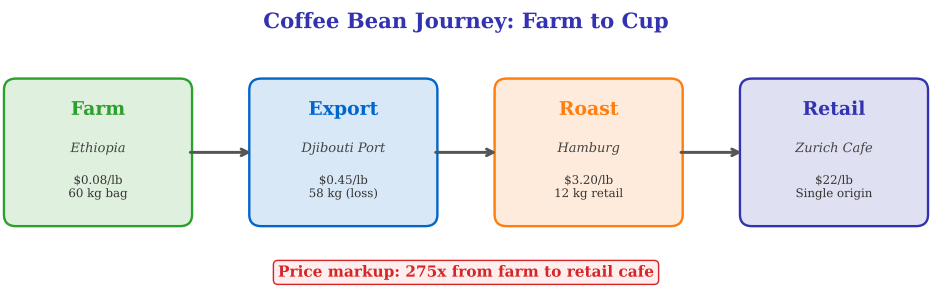
B: Somewhat — I hope so

C: Not really

D: Labels are meaningless

EU organic certification requires annual inspections, but auditors visit only 5% of certified farms. Trust depends on sample-based verification.

The Coffee Journey: 4 Handoffs, 275× Markup



Source: ICO Coffee Development Report, 2023

What you see: four-step flow from farm ($0.08/lb) through export, roasting, to retail ($22/lb). Each handoff is a trust boundary.

Why Supply Chains Are Opaque

Structural reasons:

1. **Fragmentation:** A smartphone contains 200+ components from 60+ suppliers across 30+ countries
2. **Asymmetric incentives:** Middlemen profit from opacity
3. **Paper-based records:** Bills of lading, certificates of origin, phytosanitary certificates — all forgeable
4. **Jurisdictional gaps:** No single regulator oversees cross-border chains

Economic reasons:

- **Information asymmetry** = market power
- Traceability costs money — who pays?
- "Good enough" quality hides behind brand trust
- Consumers rarely investigate beyond the label

Akerlof's Lemons Problem

When buyers cannot distinguish quality, **bad products drive out good ones**. Sellers of genuine products exit the market because they cannot recover their costs.

George Akerlof won the 2001 Nobel Prize in Economics for demonstrating how information asymmetry leads to market failure.

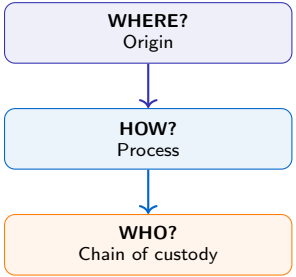
What Is Provenance?

Provenance (from French *provenir*, "to come from"):

- The **complete history** of a product: where it was made, by whom, under what conditions, through which hands it passed
- In art: "chain of custody" from artist to current owner
- In supply chains: **verifiable record of every transformation and handoff**

Three questions provenance must answer:

1. **Origin:** Where was this made? (geography, farm, mine)
2. **Process:** How was it made? (organic, fair trade, conflict-free)
3. **Chain of custody:** Who handled it? (every intermediary)



Traditional provenance relies on paper certificates and trust in intermediaries. Blockchain provenance replaces trust with cryptographic verification.

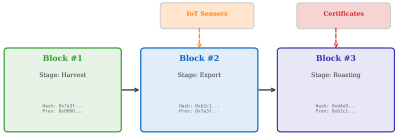
Each Handoff = One Blockchain Transaction

Core principle: Every time a product changes hands, the new custodian records the transfer on a blockchain.

What gets recorded:

- **Who:** Sender and receiver wallet addresses
- **What:** Product ID, batch number, weight
- **When:** Timestamp (block time)
- **Where:** GPS coordinates (if IoT-enabled)
- **Conditions:** Temperature, humidity (if sensor data available)

Result: An immutable, timestamped, auditable record of the product's journey.

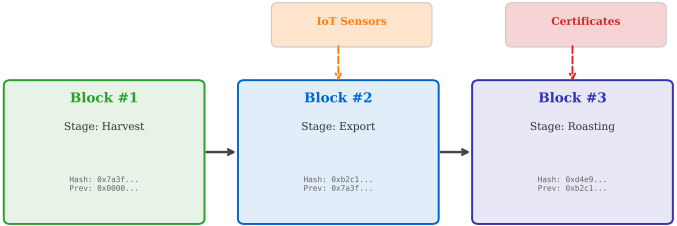


Each handoff = one block. IoT data and certificates feed in as inputs.

Immutable chain links every stage of the supply chain.

What you see: three blocks linked by hashes, with IoT sensor data and certificates feeding into specific blocks as inputs.

The Block Chain Structure — Supply Chain Edition



Each handoff = one block. IoT data and certificates feed in as inputs.

Immutable chain links every stage of the supply chain.

Key properties:

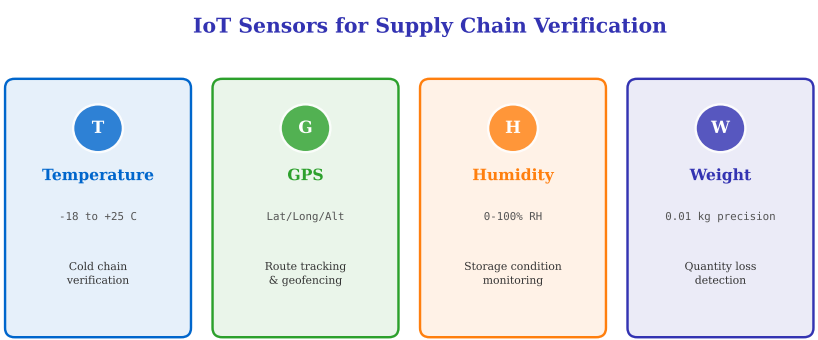
- Each block's hash includes the previous block's hash
- Tampering with Block #1 invalidates #2 and #3
- IoT data recorded automatically (no human entry)

For supply chains, this means:

- Cannot retroactively change harvest data
- Export weights permanently linked to harvest weights
- Every discrepancy visible to all participants

Hash linkage is the same mechanism used in Bitcoin (Module 3, Lesson 1). Here it secures product history instead of financial history.

IoT Sensors: Bridging Physical and Digital



What you see: four sensor types (temperature, GPS, humidity, weight) with their specifications and supply chain use cases.

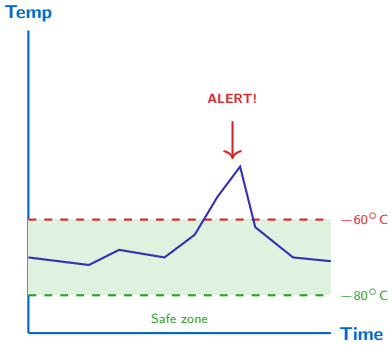
IoT in Practice: The Cold Chain

Cold chain monitoring example:

1. Vaccine leaves factory at -70°C (Pfizer COVID-19)
2. IoT sensor in shipping container records temperature every 30 seconds
3. Data is hashed and written to blockchain every 5 minutes
4. At customs, the entire temperature log is verifiable on-chain
5. **Any excursion above -60°C triggers an automatic alert**

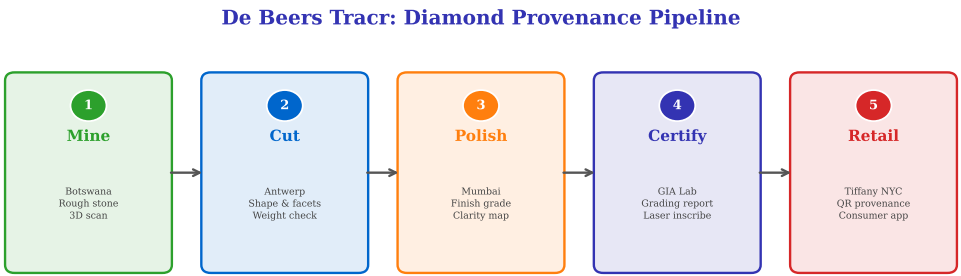
Without IoT:

- Paper logs filled in retrospectively ("I checked at 3pm")
- No evidence of conditions between checks
- Fraudulent records trivially easy to create



Pfizer's COVID-19 vaccine required -70°C storage. IoT-enabled thermal containers with blockchain logging were deployed in 80+ countries.

Case Study: De Beers Tracr — Diamond Provenance



Every diamond gets a unique digital twin on a private blockchain

Source: De Beers Group, Tracr platform (launched 2022)

What you see: five-stage pipeline (Mine, Cut, Polish, Certify, Retail) showing De Beers' diamond digital twin system launched in 2022.

Tracr Deep Dive: How a Diamond Gets a Digital Twin

Step 1 — Mine (Botswana):

- Rough stone is **3D-scanned** to create a unique digital fingerprint
- Weight, colour, inclusion map recorded
- Digital twin created on Tracr blockchain

Step 2–3 — Cut & Polish (Antwerp, Mumbai):

- Each transformation updates the digital twin
- Weight loss during cutting is tracked (rough → polished loses 50–60%)
- **Anomalous weight retention** flags potential stone substitution

Step 4–5 — Certify & Retail:

- GIA grading report linked to digital twin
- Laser inscription matches physical stone to blockchain record
- Consumer scans QR code at Tiffany to see full provenance

Tracr by the Numbers

- Launched: 2022
- Diamonds tracked: 75,000+
- Blockchain: private
- Partners: 30+ manufacturers
- Value tracked: $2B+

Limitation:
Only De Beers mines — does not cover artisanal or Russian diamonds

Tracr uses a private permissioned blockchain. The 3D scan creates a "diamond fingerprint" unique to each stone's crystal structure.

Worked Example: Ahmed's Coffee — 4 Key Handoffs

Handoff 1 — Farm → Cooperative:

- Ahmed delivers 60 kg bag to cooperative
- Bag weighed on IoT-enabled scale: **60.2 kg**
- GPS coordinates: Sidamo, Ethiopia
- Block #1 written to blockchain

Handoff 2 — Cooperative → Exporter:

- Cooperative aggregates 500 bags, ships to Djibouti
- Each bag has RFID tag linked to blockchain ID
- Arrival weight: **58.8 kg** (1.4 kg moisture loss)
- Block #2 records weight delta and transit conditions

Handoff 3 — Exporter → Roaster (Hamburg):

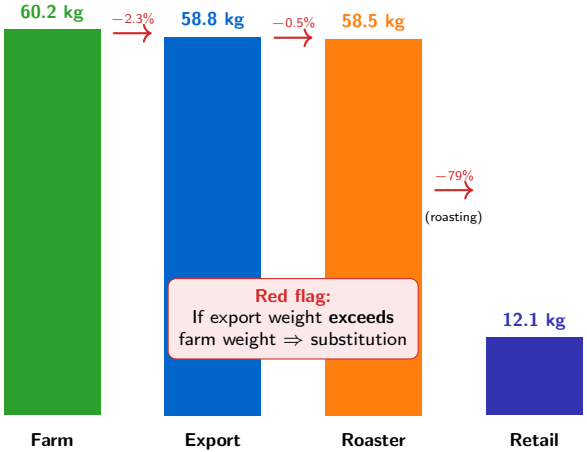
- Container arrives via Maersk (bill of lading linked)
- Temperature during 12-day voyage: 18–22°C (on-chain)
- Weight at port: **58.5 kg** (0.3 kg further loss)
- Roaster verifies origin by scanning QR on bag

Handoff 4 — Roaster → Retailer (Zurich):

- 58.5 kg green beans → **12.1 kg** roasted retail packs
- Weight loss is 79% (water + chaff) — expected range verified
- Each 250g pack gets unique QR linking to full journey
- Consumer scans: sees Ahmed's farm, transit temps, roast date

Weight tracking across handoffs is the simplest fraud-detection mechanism: unexplained weight gains indicate product substitution.

Weight Tracking as Fraud Detection



Expected losses:
Farm → Export: 1–3%
Export → Roast: 0–1%
Roast loss: 75–82%

Weight is physical and hard to fake at scale. Unexplained weight gains between handoffs are the most reliable indicator of product substitution.

Platform Comparison: Who Is Building This?

Supply Chain Provenance Platforms

Platform	Blockchain	Industry	Status
IBM Food Trust	Hyperledger (private)	Food & Grocery	Shut down 2023
VeChain	VeChainThor (public)	Luxury, Wine, Logistics	Active (China focus)
LVMH Aura	ConsenSys Quorum (private)	Luxury Goods (LVMH brands)	Active (consortium)
De Beers Tracr	Private permissioned	Diamonds	Active (industry std)

IBM Food Trust shutdown (Jan 2023) shows enterprise blockchain adoption challenges

What you see: comparison of IBM Food Trust (shut down 2023), VeChain, LVMH Aura, and De Beers Tracr across blockchain type, industry, and status.

IBM Food Trust: A Post-Mortem

What it was:

- Launched 2018 with Walmart as anchor customer
- Hyperledger Fabric (private, permissioned blockchain)
- Tracked leafy greens, seafood, pork across supply chains
- Reduced Walmart's mango trace time from **7 days to 2.2 seconds**

Why it failed (shut down January 2023):

1. **Network effect problem:** Required all participants to join — small suppliers resisted
2. **Cost:** \$10K–\$50K/year per participant — prohibitive for small farms
3. **Chicken-and-egg:** Value only emerges with critical mass of participants
4. **Competing platforms:** Each retailer wanted its own system

Key Lesson

Technology worked perfectly.

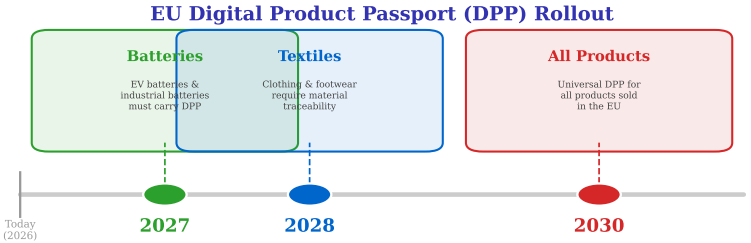
Business model failed.

Adoption requires:
- Low entry cost
- Immediate ROI
- Industry-wide standards

None of these existed.

IBM Food Trust is the most important failure case in blockchain provenance. The technology succeeded; the economics did not.

EU Digital Product Passport (DPP)



Source: EU Ecodesign for Sustainable Products Regulation (ESPR), 2024

What it requires:

- Every product sold in the EU must carry a **machine-readable digital passport** (origin, materials, carbon footprint, repairability)
- Regulators, consumers, and recyclers all get access (different data views)
- Does not mandate blockchain — but blockchain is the leading candidate

What you see: EU DPP rollout timeline — batteries (2027), textiles (2028), all products (2030). Based on EU ESPR regulation adopted 2024.

DPP: What Changes for Companies

Required data per product:

1. **Material composition** (exact percentages)
2. **Carbon footprint** (lifecycle assessment)
3. **Country of origin** (per component)
4. **Repairability score** (0–10 scale)
5. **Recycling instructions**
6. **Compliance certifications**

Scale: Applies to **every product** sold in the EU by 2030.

Implementation challenge:

- Companies must collect data from **entire supplier network**
- Small suppliers (Tier 3, Tier 4) often lack digital infrastructure
- Estimated compliance cost: €5,000–€500,000 per company
- Creates demand for **provenance-as-a-service** platforms

Regulatory Pull

Unlike IBM Food Trust (market push), the EU DPP creates **regulatory pull** — compliance is mandatory, not optional.

The EU DPP may succeed where IBM Food Trust failed because participation is legally required, solving the chicken-and-egg adoption problem.

Think-Pair-Share: Design Your Provenance System

You run a chocolate company sourcing cocoa from Ghana.

Think (2 min)

What data would you record at each handoff?

Which sensors would you deploy?

Who pays for the infrastructure?

Pair (3 min)

Compare your design with your neighbour's.

Where do you disagree?

What did you miss?

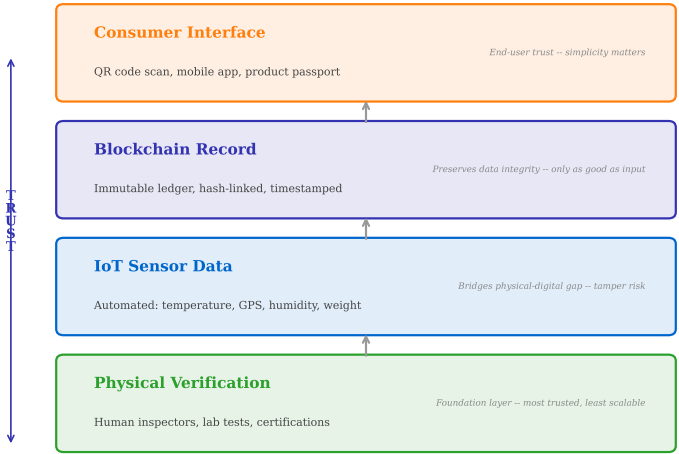
Share (5 min)

Present your design to the class.

How would you handle smallholder farmers who lack smartphones?

Cocoa supply chains involve 5–6 million smallholder farmers, most earning under $2/day. Your design must account for this economic reality.

The Supply Chain Trust Stack



What you see: four layers from physical verification (bottom) through IoT data and blockchain record to consumer QR interface (top).

Trust Stack: Each Layer Depends on the One Below

Layer 1 — Physical Verification:

- Human inspectors, lab tests, certifications
- **Most trusted** but least scalable
- Cost: $500–$5,000 per inspection

Layer 2 — IoT Sensor Data:

- Automated: temperature, GPS, humidity, weight
- Continuous monitoring (every 30s)
- **But:** sensors can be tampered with

Layer 3 — Blockchain Record:

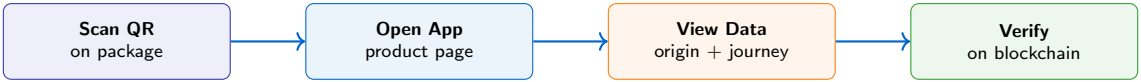
- Immutable, timestamped, hash-linked
- **But:** only as trustworthy as data entered
- "Garbage in, garbage out" — permanently

Layer 4 — Consumer Interface:

- QR code → app → product history
- **But:** QR on fake product links to real product's history
- The "last mile" trust problem

The trust stack is only as strong as its weakest layer. In most supply chains today, Layer 1 (physical verification) remains the weakest link.

From QR Code to Full Provenance — Consumer View



What the consumer sees:

Origin	**Journey**	**Certifications**	**Blockchain proof**
Farm name, GPS, farmer photo	4 handoffs, dates, transit conditions	Organic, Fair Trade, Rainforest Alliance	Transaction hash, block number

Consumer-facing provenance apps (e.g., Provenance.org, OpenSC) show this information. Few consumers actually check the blockchain hash.

Worked Formula: Hash Chain Verification

How do you verify that a provenance record has not been tampered with?

Step 1: Each handoff produces a data packet D_i:

$$D_i = (\text{sender}_i, \text{receiver}_i, \text{weight}_i, \text{GPS}_i, \text{timestamp}_i)$$

Step 2: Hash the data packet with the previous hash:

$$H_i = \text{SHA-256}(D_i \,||\, H_{i-1})$$

Step 3: For genesis (first handoff): $H_0 = \text{SHA-256}(D_0 \,||\, 0\text{x}0000...)$

Verification

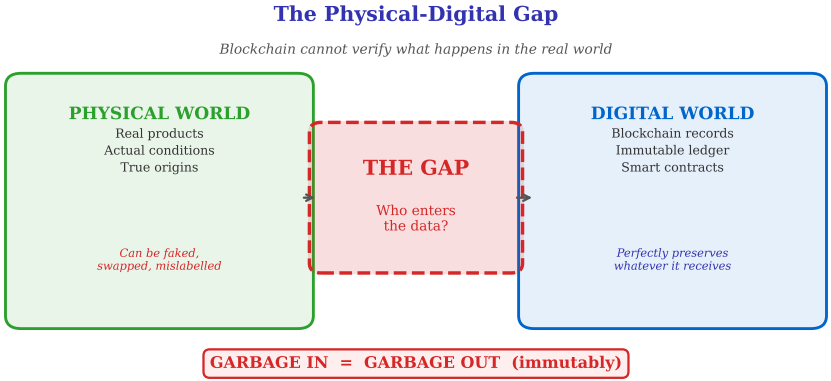
To verify handoff #3, recompute:

$$H_3' = \text{SHA-256}(D_3 \,||\, H_2)$$

If $H_3' = H_3$ on chain $\Rightarrow$ data at handoff #3 is untampered.
If $H_3' \neq H_3 \Rightarrow$ either D_3 or H_2 was modified $\Rightarrow$ **flag for investigation**.

This is the same hash-chain mechanism from Lesson 1 (cryptographic foundations). Supply chain provenance is a direct application of hash chaining.

The Physical-Digital Gap



What you see: Physical World and Digital World separated by "THE GAP" — who enters the data? Garbage in = garbage out, immutably.

Garbage In = Garbage Out (Immutably)

The fundamental limitation:

- Blockchain secures **data integrity** (what was recorded cannot be changed)
- Blockchain does **not** secure **data accuracy** (what was recorded may be false)
- Someone must type "organic" into the system — the blockchain cannot verify the soil

Real-world examples:

1. Farmer enters "pesticide-free" — blockchain records it immutably
2. Inspector visits 6 months later — finds pesticide residues
3. The blockchain now contains an **immutable lie**
4. Correction requires a new transaction — the original record persists forever

The Oracle Problem

Blockchains need external data sources ("oracles") to know about the physical world.

Who watches the oracle?

This is the trust problem *moved, not solved.*

The oracle problem is not unique to supply chains — it affects all blockchain applications that depend on real-world data (DeFi price feeds, insurance, etc.).

IoT Tampering: When Sensors Lie

Physical tampering methods:

1. **Sensor relocation:** Move GPS sensor to a different container
2. **Thermal shielding:** Wrap temperature sensor in insulation — it reads correct while product defrosts
3. **Weight manipulation:** Add water to coffee bags before weigh-in
4. **Signal jamming:** Block cellular connectivity during transit

Cost of attack: \$10–\$100
Cost of sensor: \$5–\$50

Asymmetry: Attacking is cheaper than defending.

Defences:

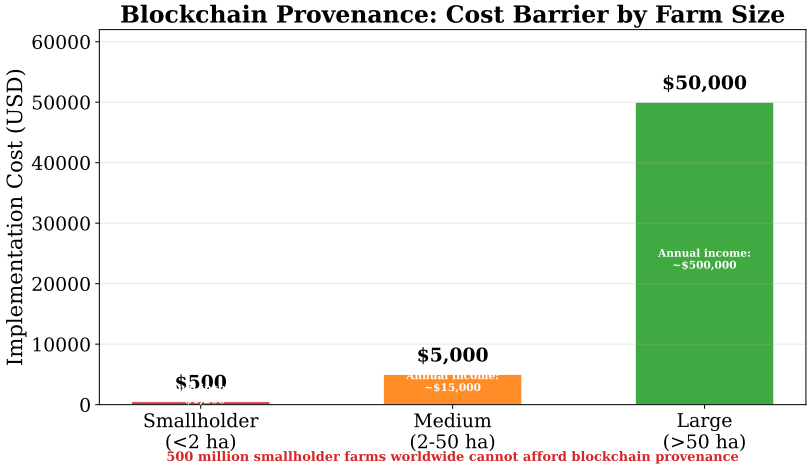
- **Tamper-evident seals:** Physical indicators that sensor was moved
- **Multi-sensor correlation:** GPS + temperature + humidity must be consistent
- **Anomaly detection:** ML models flag impossible readings (e.g., GPS jump without matching transit time)
- **Random physical audits:** Inspectors verify sensor placement

Key Insight

IoT sensors **reduce** trust requirements but do **not eliminate** them. Defence is layered, not absolute.

The sensor tamper problem parallels the speedometer fraud in used cars — technology can be manipulated when the incentive is strong enough.

The Smallholder Cost Barrier



What you see: three bars showing blockchain implementation cost by farm size — $500 (smallholder), $5K (medium), $50K (large). 500M farmers excluded.

The $500 Problem: When Provenance Excludes the Poorest

What $500 buys a smallholder farmer:

- 5 months of family food
- 2 years of children's school fees
- A dairy cow
- **Or:** basic blockchain provenance setup

The inclusion paradox:

1. Provenance systems are designed to help small farmers prove their quality
2. But small farmers cannot afford to participate
3. Large farms adopt provenance → get premium prices
4. Small farms lose market access → deeper poverty
5. **The technology designed to help them makes things worse**

Possible solutions:

- **Cooperative models:** Share infrastructure across 100+ farms
- **Mobile-first:** SMS-based entry (no smartphone required)
- **Buyer-funded:** Roasters pay for farmer provenance
- **Subsidy:** Development bank funding (World Bank, IFC)
- **Lightweight protocols:** Not every handoff needs full blockchain

Farmforce (by Syngenta) and SourceTrace use SMS-based entry to include farmers without smartphones — reaching 2M+ farmers by 2023.

Scalability vs. Granularity: The Fundamental Trade-off

Maximum granularity:

- Track every single bean, pill, or component
- Record every 30-second sensor reading
- Full provenance for every retail unit
- **Cost:** Enormous data storage, thousands of transactions per product

Real example:
A single pallet of coffee (320 bags) through 4 handoffs with 30-second IoT readings over 14 days = **322,560 data points**.

At 7 TPS (Ethereum L1): **12.8 hours** to process one pallet.

Practical compromises:

1. **Batch tracking:** Track pallets, not individual bags
2. **Aggregated IoT:** Record hourly averages, not per-second
3. **Layer-2 solutions:** Record summaries on-chain, details off-chain
4. **Merkle trees:** Hash all sensor data into one root hash per handoff

Merkle Root Approach

322,560 readings $\rightarrow$ 1 Merkle root per handoff.
4 handoffs $\rightarrow$ 4 transactions total.
Any single reading can be verified against the root.

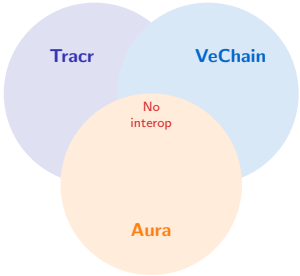
The Merkle tree approach reduces on-chain data by 99.9% while preserving verifiability. This is the same technique used in Bitcoin's SPV (Simplified Payment Verification).

The Competing Standards Problem

Current landscape:

- **GS1 EPCIS:** Industry standard for supply chain events (barcode consortium)
- **W3C DID:** Decentralized identifiers for products and actors
- **ISO 22739:** Blockchain terminology standard
- **EU DPP schema:** European Commission's data model
- **Proprietary:** Each platform (VeChain, Aura, Tracr) has its own data model

Problem: A diamond tracked on Tracr cannot be verified by a system using VeChain. Supply chains cross platform boundaries.



"The nice thing about standards is that there are so many to choose from." — Andrew Tanenbaum

Interoperability is the largest unsolved technical problem in supply chain provenance. GS1 EPCIS 2.0 (2022) is the leading candidate for a universal standard.

Privacy vs. Transparency: An Unresolved Tension

Transparency demands:

- Consumers want to see the full supply chain
- Regulators need audit access
- NGOs want labour and environmental data
- Investors want ESG compliance proof

Privacy demands:

- Suppliers don't want competitors to see their margins
- Pricing data is commercially sensitive
- Supplier relationships are trade secrets
- GDPR applies if personal data is involved

Technical solutions:

1. **Zero-knowledge proofs (ZKP):** Prove "this coffee is organic" without revealing the farm's identity or price
2. **Selective disclosure:** Different data views for consumer, regulator, and business partner
3. **Private channels:** Hyperledger Fabric allows data visible only to authorised parties
4. **Hash-only on-chain:** Full data off-chain, only hashes on public blockchain

ZKP promise: "I can prove this claim is true without showing you the evidence."

Zero-knowledge proofs are covered in detail in Module 3, Lesson 1. In supply chains, ZKPs could verify compliance without exposing business secrets.

Environmental Cost of Provenance

The irony:

- Supply chain provenance aims to prove sustainability
- But running a blockchain **consumes energy**
- IoT sensors contain **rare earth minerals**
- QR labels add **packaging waste**

Energy comparison per transaction:

- Bitcoin (PoW): **707 kWh**
- Ethereum (PoS, post-Merge): **0.03 kWh**
- Hyperledger Fabric: **0.001 kWh**
- Paper certificate: **0 kWh** (but forgeable)

Net impact analysis:

Benefits

Reduce food waste (30%)
Prevent counterfeit drugs
Prove sustainability
Enable circular economy

Costs

Blockchain energy use
IoT device e-waste
Server infrastructure
Packaging for QR labels

Verdict: If provenance reduces food waste by even 1%, the environmental benefit vastly exceeds the blockchain energy cost.

The UN estimates 1.3 billion tonnes of food is wasted annually. Provenance-enabled supply chains could reduce waste by improving inventory management.

Who Wins, Who Loses?

Winners:

- **Premium brands:** Can prove authenticity (LVMH, De Beers)
- **Large retailers:** Better recall management (Walmart)
- **Regulators:** Faster enforcement, better data
- **Consumers:** More information (if they use it)
- **Platform providers:** New SaaS revenue streams

Losers:

- **Fraudsters:** (Intended — the whole point)
- **Smallholder farmers:** Cannot afford entry cost
- **Developing-country exporters:** New compliance burden
- **Privacy-sensitive suppliers:** Forced transparency
- **Middlemen:** Reduced information advantage

The uncomfortable truth: Supply chain provenance, as currently designed, benefits those who can already afford trust infrastructure — and may further marginalise those who cannot.

Equity considerations are central to the EU DPP design. The regulation includes provisions for SME transition support, but implementation details are unclear.

Lessons from Failures

IBM Food Trust (2018–2023):

- Technology worked; business model failed
- **Lesson:** Network effects require critical mass — you cannot force adoption through one anchor customer

Everledger (diamonds, 2015–):

- Pivoted from diamonds to general provenance
- Struggled to scale beyond pilot projects
- **Lesson:** Single-industry vertical is too narrow

Walmart China (pork tracking, 2017):

- Required all pork suppliers to use VeChain blockchain
- Many small suppliers hired data-entry clerks to fabricate records
- **Lesson:** Mandating technology does not eliminate human fraud

Common patterns across failures:

1. Overestimated technology, underestimated behaviour
2. Ignored cost burden on smallest participants
3. Assumed "immutable" means "true"
4. Built for compliance, not for user value

The best provenance systems create value for every participant in the chain, not just the buyer at the end. Value alignment drives adoption.

Key Takeaways

1. **The problem is real:** $4.2T in counterfeiting, 1M+ deaths from fake medicine, systemic food fraud — supply chain opacity has lethal consequences
2. **Blockchain enables provenance:** Each handoff becomes a transaction; hash chains make records tamper-evident; IoT sensors bridge the physical-digital gap
3. **But blockchain cannot verify reality:** "Garbage in = garbage out (immutably)" — the oracle problem applies to supply chains just as it does to DeFi
4. **Economics matter more than technology:** IBM Food Trust had perfect technology and zero business model. Cost barriers exclude 500M smallholder farmers
5. **Regulation may be the catalyst:** The EU Digital Product Passport (2027–2030) creates mandatory demand for provenance infrastructure

One sentence: Supply chain provenance on blockchain is a promising partial solution to a massive trust problem — not a complete one.

Provenance is necessary but not sufficient. It must be combined with physical verification, IoT sensors, and regulatory enforcement.

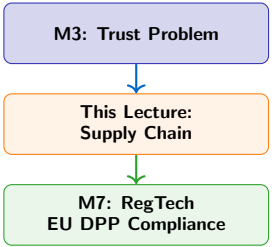
Bridge: What Comes Next

In this lecture, we explored:

- The trust problem in supply chains
- How blockchain provenance attempts to solve it
- The fundamental limitations (physical-digital gap, cost, standards)

In Module 7 (RegTech & Compliance), you will:

- Deep-dive into the EU Digital Product Passport regulation
- Learn how companies must prepare for 2027 compliance
- Explore provenance-as-a-service business models
- Analyse the regulatory technology stack for DPP implementation



The EU DPP is the most significant regulatory driver for blockchain provenance. Module 7 covers the full compliance stack.

EU Digital Product Passport launches in 2027.

Will it **reduce counterfeiting**... or just add **compliance cost**?

Optimist case:

Mandatory participation solves the chicken-and-egg problem. Universal standard emerges. Consumers gain real power.

Pessimist case:

Becomes box-ticking exercise. Small companies hire consultants to fill forms. Physical-digital gap unchanged.

This is an open research question. The EU DPP pilot programmes (2025–2026) will provide the first empirical evidence. Watch for results in your careers.

Further Reading

Academic:

- Saberi et al. (2019), "Blockchain technology and its relationships to sustainable supply chain management," *IJPR*
- Kshetri (2018), "Blockchain's roles in meeting key supply chain management objectives," *IJIM*
- Montecchi et al. (2021), "Supply chain provenance using blockchain," *SCMIJ*

Industry:

- OECD (2023), *Trade in Counterfeit Goods*
- WHO (2023), *Substandard and Falsified Medical Products*

Case studies:

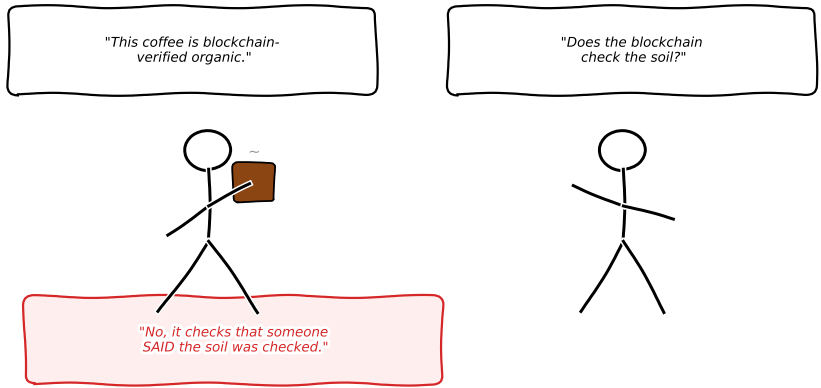
- De Beers Tracr: `tracr.com`
- VeChain: `vechain.org`
- LVMH Aura: `auraluxuryblockchain.com`
- EU DPP: `ec.europa.eu/ecodesign-dpp`

Failure analysis:

- IBM Food Trust shutdown coverage (CoinDesk, Jan 2023)
- UC Davis olive oil study (2011, updated 2020)

Start with Saberi et al. (2019) for a systematic literature review. The OECD report provides the most comprehensive counterfeiting data.

Final Thought



Immutable records of unverified claims are still unverified claims.

Blockchain is a tool for recording trust, not a substitute for creating it. The soil still needs to be checked by someone.

Appendix A: TradeLens — The Largest Shipping-Blockchain Shutdown

The IBM Food Trust post-mortem is on Slide 21. The bigger story — by transaction volume and commercial scale — is TradeLens. It must be part of any honest blockchain-in-supply-chain curriculum.

TradeLens (2018–2023) — the numbers that mattered

- **Founders:** Maersk (world's largest container-shipping line) + IBM; launched Aug 2018 on Hyperledger Fabric
- **Scope:** digitise bills of lading, customs filings, and shipping documents across the global container-logistics network
- **Scale at peak:** ∼300+ ecosystem members (*Maersk TradeLens press archive 2022*, 2022); handled an estimated 50%+ of global ocean-container shipping data (*IBM TradeLens factsheet 2022*, 2022) at times
- **Nov 29, 2022:** Maersk + IBM jointly announced wind-down. Production data services terminated Q1 2023 (*Maersk press release, Nov 29 2022*, 2022)

Root causes (per Maersk's own statement):

- **"The need for full global industry collaboration has not been achieved."** Rival shipping lines (MSC, CMA CGM, Hapag-Lloyd) were unwilling to route their commercial data through a platform co-owned by their largest competitor.
- "A viable business model" could not be established as a **neutral industry platform**
- The technical platform worked; the **governance and competitive dynamics did not**

Why this is pedagogically central: TradeLens is the largest deployment-then-shutdown of a permissioned industry blockchain — and by container-volume coverage, it was ∼100× the scale of IBM Food Trust. If a blockchain consortium co-led by the world's largest shipping company could not get rivals to join, the "neutral consortium blockchain" business model in logistics is structurally hard. Technology was never the constraint.

Source: Maersk press release Nov 29, 2022 ("A.P. Moller – Maersk and IBM to discontinue TradeLens"). The single most important missing case from any blockchain-in-shipping curriculum. Gartner's 2023 Blockchain Hype Cycle placed "blockchain in supply chain" firmly in the Trough of Disillusionment partly on this evidence.

Appendix B: Why Blockchain Often Doesn't Fit Supply Chain

Slide 21 (Food Trust) and Appendix A (TradeLens) are the failure cases. Here is the structural pattern behind both.

The "last mile" trust gap

- Blockchain records what someone *wrote* on-chain — not what actually happened in the warehouse
- An olive-oil bottle with a QR code can still be refilled with sunflower oil
- RFID tags can be cloned; IoT sensors can be bribed or tampered
- "Garbage in, garbage out" — immutably

The oracle problem, supply-chain edition

- Every on-chain handoff requires an off-chain human or sensor to sign an attestation
- That signer is the trust bottleneck — the chain does not verify reality
- Cost of deploying and auditing those signers across 500M smallholder farmers (*FAO Smallholder Farmers Report 2022*, 2022) is prohibitive

Permissioned chains ≈ distributed database

- If every writer must be pre-authorised (consortium chain), you have a shared database with hash linking — **not a blockchain's security model**
- A well-run PostgreSQL with signed append-only tables gives you 90% of the auditability at 1% of the integration cost
- Gartner 2023 Hype Cycle: "Blockchain in Supply Chain" moved into the **Trough of Disillusionment**

The narrow niche where it does fit

- Cross-jurisdiction provenance where no single authority has standing (e.g., conflict minerals, carbon credits)
- Regulatory-mandated shared infrastructure (EU Digital Product Passport, 2027–30)
- Verifiable-credential issuance for individual products with physical-digital binding and expensive counterfeiting

The honest reading: a blockchain fixes the database layer. It does not fix the "was this olive oil actually cold-pressed in Tuscany" layer. That's a human problem, and always will be. Source: Saberi et al. (2019); Gartner Hype Cycle for Blockchain 2023.