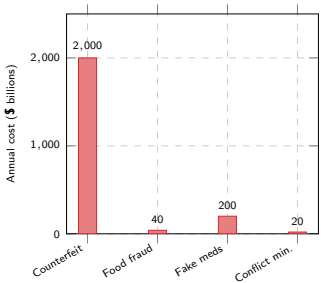
Why can you not trust that what you buy is what it claims to be?

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

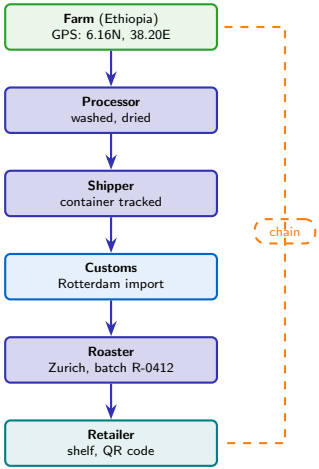
Key insight: The longer the supply chain, the more opportunities for fraud — and the harder it is to verify authenticity.

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.

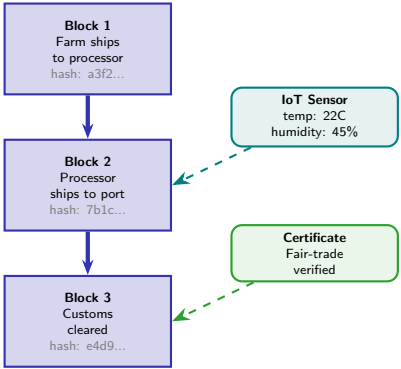
The promise: Every handoff recorded, every claim verifiable, every certificate unforgeable.

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.

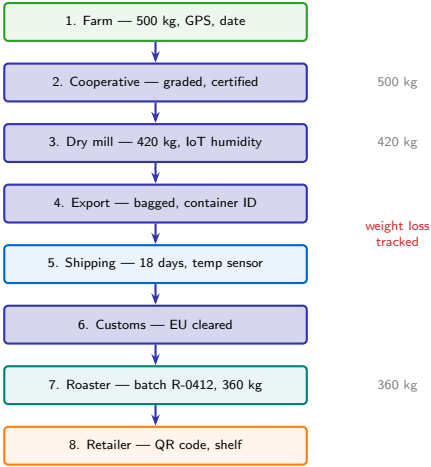
5. Shipping: Djibouti to Rotterdam. Temperature sensor: max 24C. Transit: 18 days.

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):

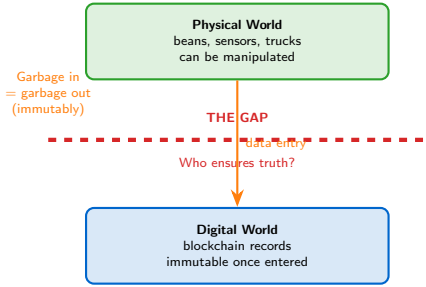
- Blockchain guarantees that records cannot be changed after entry
- But it *cannot* guarantee that the data entered is correct
- If a farmer registers conventional beans as organic, the blockchain will faithfully record a lie

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:

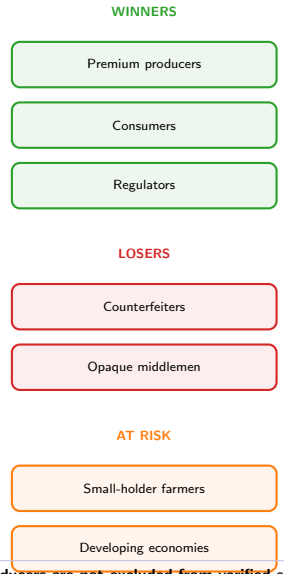
- **Premium producers:** can prove origin and quality, charge premium
- **Consumers:** can verify claims (organic, fair-trade, conflict-free)
- **Regulators:** real-time audit trails replace periodic inspections
- **Brands:** protect reputation by proving authenticity

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*