OpenEPCIS

Fascinating in Theory. It Just Doesn't Work in Practice.

Why blockchain is the wrong answer to traceability, and why it refuses to die anyway.

Sven Böckelmann · 19 June 2026 · 16 min read

blockchain • traceability • dpp • epcis • verifiable-credentials • gs1 • supply-chain • iot

openepcis.io/blog/blockchain-traceability

Contents

The one question almost nobody asks . . . 3
The consortium that wasn't . . . 3
The immutability of a lie . . . 4
The bodies in the basement . . . 5
The GDPR problem . . . 5
If the real data sits beside the chain, what is the chain for? . . . 5
What actually works . . . 6
Where blockchain genuinely earns its place . . . 7
And then there's IoT . . . 7
So why won't it die? . . . 8
Where the chain truly belongs . . . 9
Bottom line . . . 9
Sources . . . 9

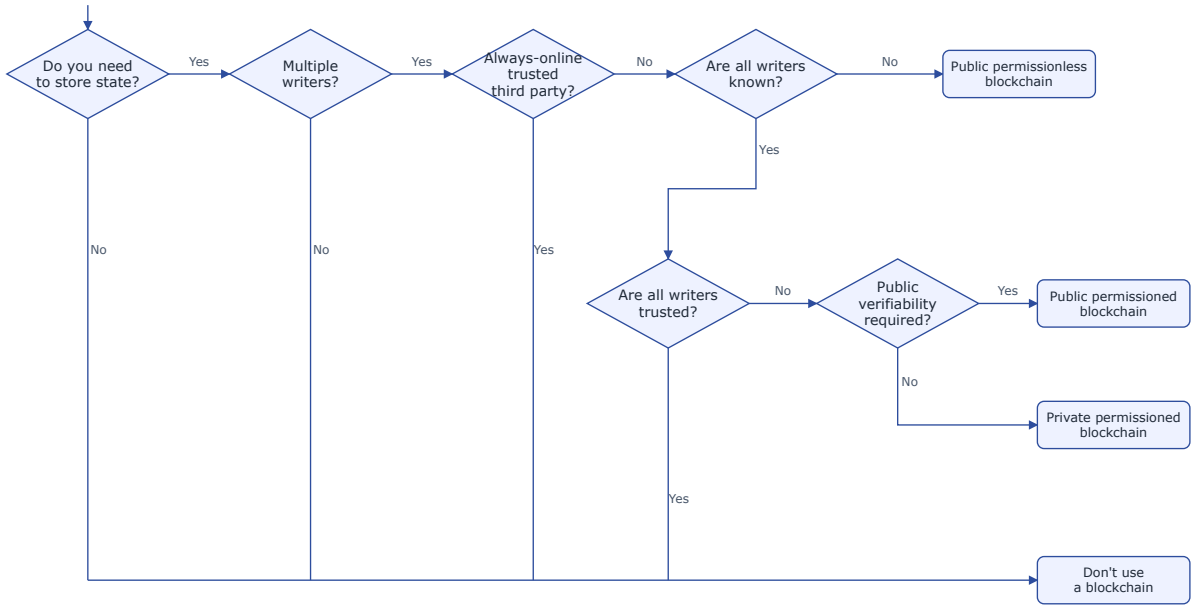
Why blockchain is the wrong answer to traceability, and why it refuses to die anyway.

There is a Pavlovian reflex in our industry. Someone says "traceability," and the next sentence says "blockchain." Track and trace, supply chain, Digital Product Passport, and out comes the ledger. Or whatever this season's word for it happens to be. Same procedure as every year. Fascinating, no question. It just doesn't work.

I want to explain why the technology is the wrong choice for this job, why it keeps coming back like something undead, and to check honestly whether I have a blind spot. If there were a reason that made blockchain indispensable for traceability, I would want to know it.

The one question almost nobody asks

In 2018, Karl Wüst of ETH Zurich and Arthur Gervais of Imperial College London published a decision diagram that fits the entire debate onto a single page. Do you need a blockchain? Only when four things come together: you need to store state, there are multiple writers, there is no always-online trusted third party available, and the writers do not trust one another.



The paper puts it cleanly. If a trusted third party is available that does not need to be permanently online, it can establish a known group of writers and function as a certificate authority. Classic PKI is enough.

Hold that against a real supply chain. The participants are known, with GS1 identifiers, contracts, regulators, certifiers, customs authorities, trade registries, and inspection bodies. These are precisely the trusted authorities whose absence would justify a blockchain in the first place. The core condition fails. The diagram's answer is clear: no blockchain.

Blockchain solves a trust problem between anonymous, mutually distrusting parties with no referee. A regulated supply chain has known parties under contract and oversight. The match is wrong from the start.

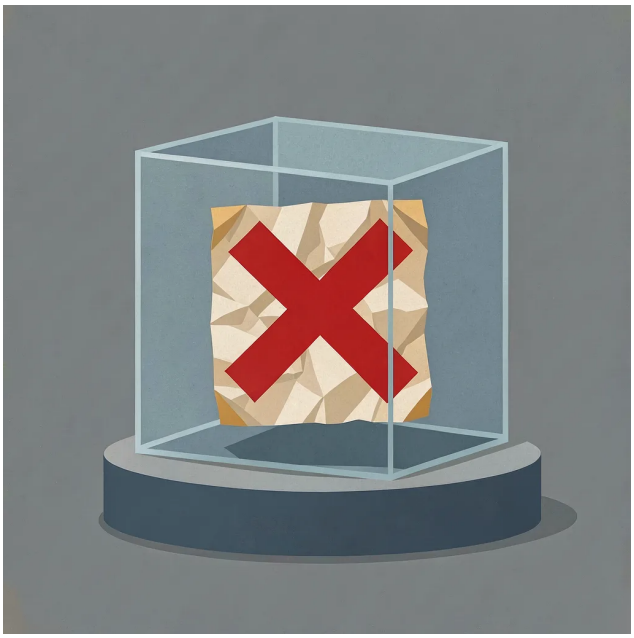
The consortium that wasn't

The usual rescue is to say that public blockchain doesn't fit, but a permissioned consortium chain does. This is where the argument gets quietly absurd. A permissioned blockchain run by one

operator with a hand-picked set of nodes is a distributed database wearing a costume. Once the writers are known and bound by rules, the consensus ceremony adds no security that a signed database with access control doesn't already provide.

TradeLens is the textbook case. It ran on Hyperledger Fabric, Maersk controlled the platform, and its competitors stayed out for exactly that reason. The chain did not solve the trust problem, because the chain was the trust problem. When one operator effectively controls the ledger, calling it a blockchain is marketing language.

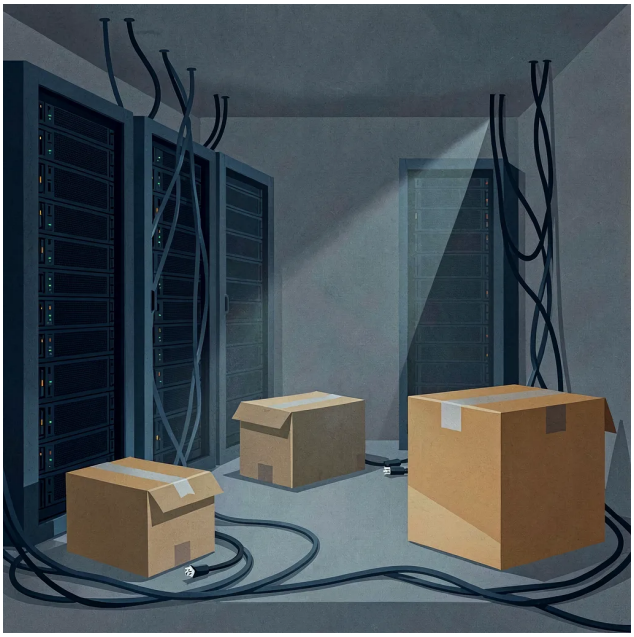
The immutability of a lie



Suppose you ignore all of that. Then comes the argument that cannot be waved away. A blockchain guarantees that data cannot be changed after it is written. It says nothing about whether the data was true when it was written.

The temperature of a cold chain is measured by whoever is holding the goods at that moment. Whether the mango really comes from the region listed in the record, the chain cannot know. It knows only what someone entered into it. Garbage in, garbage out, and at the end you have a tamper-proof copy of a false claim. The World Economic Forum says so in its own blockchain toolkit: if the data is not accurate to begin with, making it immutable on a blockchain provides no benefit.

The bodies in the basement



Theory is one thing. Look at the record.

TradeLens, the flagship from IBM and Maersk, launched in August 2018. By 2020 it had more than 175 organizations and data from over 600 ports. Shutdown was announced in November 2022, and the platform was offline by the end of Q1 2023. Maersk said it had not reached commercial viability. Lars Jensen of Vespucci Maritime put the lesson plainly on LinkedIn: what determined the fate of TradeLens was commercial usage, and the sophistication of the technology was beside the point.

IBM Food Trust and the famous mango test, nearly seven days of manual traceback reduced to 2.2 seconds with blockchain. The number has done the rounds for years. It came from a single pilot at a single retailer, and any EPCIS database with GS1 keys delivers the same speedup, without a consensus mechanism.

Everledger, the diamond pioneer, took $20M from a Tencent-led round in 2019. A follow-on deal in late 2022 fell apart when the conditional balance never arrived. By 2023 the company had wound down, its Australian subsidiary in administration and the UK entity in liquidation.

The pattern repeats. Big launch, grant money, pilots, then silence. The technology was well built. The job was the wrong one for it.

The GDPR problem

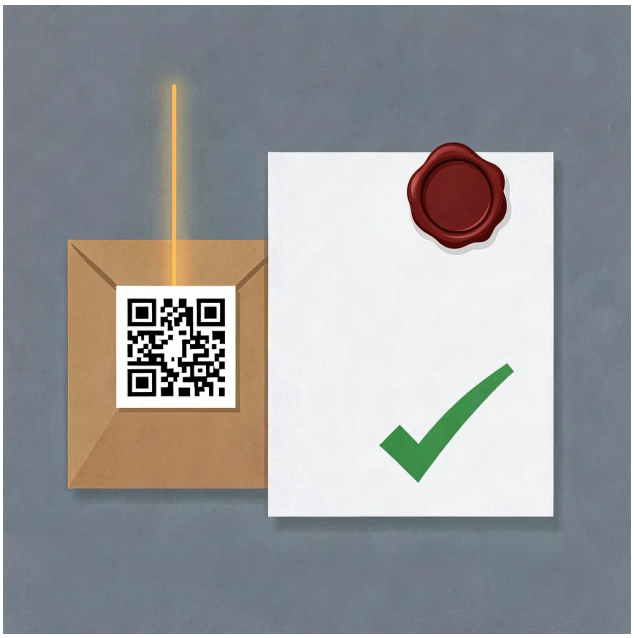
Immutability sounds like a virtue until personal data enters the picture. Article 17 GDPR, the right to erasure. Article 16, the right to rectification. A blockchain is built on purpose so that later changes are hard or impossible. The EDPB Guidelines 02/2025 spell out the structural conflict and tell controllers to keep personal data off-chain, with only hashes or references on the chain. The same guidelines caution that even those hashes can themselves be personal data, so the chain never fully escapes the regulation. Which brings us to the next point.

If the real data sits beside the chain, what is the chain for?

The honest answer to scaling is Merkle batching. Only hashes go on the chain, and the data lives in a system beside it that holds it, signs it, and serves queries. Once that off-chain system is doing all the work, EPCIS 2.0 plus signed credentials covers everything, and the chain adds nothing that a signed, timestamped data structure does not already provide.

For high-value single items the overhead may pay off. For everyday consumer goods, billions of items, thin margins, and constant churn through returns, repair, refurbishment, and recycling, it does not. Permissioned chains hit the throughput numbers by collapsing into a centrally-operated database that happens to be running Fabric underneath. The economics never carry for thin-margin mass goods. A realistic estimate is around 25 dollars per container per journey, about one percent of average container transport cost. Tolerable for container freight. Absurd for a single pair of jeans on a shelf.

What actually works



The alternative exists, it is standardized, and it runs in production today.

Verifiable Credentials let a known issuer make a signed, machine-readable statement about a product. A verifier checks it locally, offline, with no global consensus and no transaction cost. Selective disclosure through SD-JWT protects confidential business data. Issuer identity resolves through ledger-free DID methods such as did:web or did:key. If you want a verifiable history, did:webvh delivers one, again without a ledger.

Beneath that sits the real infrastructure. GS1 EPCIS 2.0 as the standardized event model for the what, when, where, and why. GS1 Digital Link, which connects the physical product to its passport through a QR code, the same code for the checkout and for the consumer. GS1 Web Vocabulary and JSON-LD for the semantics. The UN Transparency Protocol from UNECE issues all of its credentials as W3C Verifiable Credentials and describes GS1 EPCIS 2.0 as a mature, widely deployed standard.

Regulation points the same way. The EUDI wallet under eIDAS 2.0 builds its trust model on X.509 certificates and classical certificate authorities. DIDs and blockchain are not mandated; the formal request to include DIDs in the ARF had to be filed by the Decentralized Identity Foundation, the Digital Credentials Consortium, and the Trust Over IP Foundation, which is itself the clearest signal that they remain optional. Microsoft removed did:ion from Entra Verified ID in December 2023, with did:web as the recommended default. On 27 May 2026, CEN and CENELEC published the first EN standards for the EU DPP, the EN 182xx series from technical committee JTC 24, written to be system-agnostic and vendor-independent. GS1 itself, in GS1 Standards enabling the EU digital product passport, recommends Verifiable Credentials for integrity and treats blockchain as just one option, "entirely a choice for industry."

The technology is settled. The standards are published. The implementations are deployed. There

is no gap that a chain is needed to fill. And none of it is a blockchain, however often the label gets pinned to signed credentials by vendors who know the word still moves budget.

Where blockchain genuinely earns its place

I do not want to make this too easy on myself. Good practice for traceability is the previous section, full stop. But there are niches, well outside it, where the chain is at least defensible, and anyone who talks them away leaves an opening. So here is the honest accounting of that thin edge.

Genuinely adversarial settings with no trusted authority at all. This is the Wüst and Gervais condition exactly, and in regulated supply chains the authority exists.

Censorship resistance and the absence of a single point of control. Real and relevant in sanctions evasion. For a consumer product passport, censorship resistance is not a design goal, and the manufacturer is meant to be the authoritative source.

Timestamping and proof of existence through hash anchoring. The most common residual claim, and the thinnest. RFC 3161 timestamping under eIDAS, with audited time-stamping authorities operating to ETSI EN 319 421 for policy and security requirements and ETSI EN 319 422 for the protocol and token profile, delivers a qualified timestamp with a legal presumption of accuracy and integrity, and only the hash leaves the client. Append-only public logs such as Certificate Transparency and Sigstore Rekor give equivalent tamper-evident existence proofs where public visibility is the design goal. All of it at internet scale today, without a consensus ledger.

Tokenization of high-value assets is where the case looks strongest. De Beers Tracr is running, with more than five million rough diamonds registered at source, around two-thirds of De Beers' production by value, and GIA announced a 30% stake in May 2026. It is a real deployment, and the definition of a niche, where the per-item value carries the overhead. Even here the chain is thinner than it looks. The records that matter are written and vouched for by De Beers, so the trust still rests on De Beers' own ledger. By the same argument that sank the consortium chains, a single authoritative writer makes the consensus ceremony optional. The everyday goods of the mass DPP are nowhere near this value anyway, so the example supports the thesis more than it weakens it.

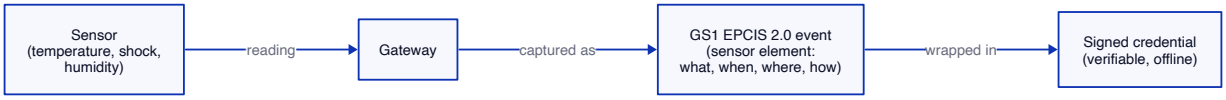
Automated settlement and supply chain finance. A financial use case where information lives on the chain itself, with no outside reality to second-guess. Traceability is a separate problem with a separate answer.

After honest review, the blind spot is real and small, and it sits outside the area in question. None of these niches makes blockchain necessary for mass traceability, for the passport of everyday goods, or for the circular economy.

And then there's IoT

The same reflex has a sibling. Put a sensor in everything, the pitch goes, and the supply chain turns transparent on its own. Sensors are genuinely useful where a product's condition can change in transit, a vaccine warming or a crate taking a knock, but a reading is only a measurement, and only as honest as whoever placed the device. It is also nothing new. GS1 EPCIS 2.0 added a dimension for exactly this, the "how" of an event, so a temperature or humidity reading rides inside the same standardised event as the what, when and where, ratified as ISO/IEC 19987:2024. Sensors are one more kind of data flowing into the boring stack, which absorbed them years ago.

So should the sensor data go on a blockchain? This is where the two fashions meet, and the meeting makes both worse. Immutability does nothing for a reading whose honesty depends on where the probe was clipped. It just freezes a possibly false number in place forever. A cold chain also produces a constant stream of readings, the heaviest and most repetitive data imaginable, which is the worst possible fit for an append-only ledger that every node has to store and replicate. Put personal or commercially sensitive data in that stream and the erasure problem from earlier comes straight back. Sign the reading and attach it to an EPCIS event, and you get an integrity guarantee that stands up in court without asking a thousand machines to keep a copy of last Tuesday's fridge temperature.



So why won't it die?

Because a legitimate wish gets equated, by reflex, with one technology. The word itself has stretched until it covers anything cryptographic, the same drift now playing out with AI, where every product that touches a file becomes AI-powered and auditors, regulators, and procurement teams wave it through because the language is fuzzy enough to allow it. People want immutability, transparency, and trust, and they say "blockchain," even though signed data structures, append-only logs, and PKI deliver exactly that without the consensus overhead. Add consulting and platform revenue and a healthy dose of fear of missing out.

And there is the quiet engine. Blockchain and traceability have fused in the minds of the people who fund and steer the work. The EU Blockchain Observatory gave the Digital Product Passport its own report, a blockchain-based perspective, folding even verifiable credentials and DIDs into the blockchain story, while conceding that no regulation prescribes a chain. Want the grant? Propose the chain, whether or not it is the right tool. The output is real: papers, prototypes, conference slots. The deployments are not. The research records it soberly: many publications, very little production use.

Where the chain truly belongs

There is one place the chain genuinely shines, and it has nothing to do with any of this: money. When your own currency is melting and the government behind it is the cause, a token that moves value out of its reach stops being a toy and becomes a lifeline. The most grassroots adoption sits in emerging markets and runs largely on stablecoins, people reaching for the dollar over crypto rails because their own money will not hold. High-risk but real, and a story about money, with nothing to teach the passport of a pair of jeans.

Bottom line

Traceability needs verifiable, signed statements from known issuers, checkable locally, selectively disclosable, and erasable. Verifiable Credentials, DIDs, and GS1 EPCIS 2.0 deliver all of that in full.

Blockchain addresses a trust problem that regulated supply chains do not have. The economics do not carry for thin-margin mass goods. Where personal data is involved, it collides with Article 17 GDPR. Where one operator controls the ledger, calling it a blockchain is marketing language. And it never establishes the truth of what was recorded. The chain only preserves it.

One test would change my mind. Show me a production system, not a pilot, that closes the gap between physical reality and the recorded data without an off-chain trust anchor, stays GDPR compliant without offloading the real data, and costs less per event for thin-margin mass goods than credentials and EPCIS. Until then it holds: fascinating in theory, and it just doesn't work in practice.

So when are we finally going to drop the blockchain nonsense?

Sources

Foundational paper - Karl Wüst and Arthur Gervais, "Do you need a Blockchain?", CVCBT 2018: https://www.law.berkeley.edu/wp-content/uploads/2018/08/Do-you-need-a-Blockchain-Karl-Wust-and-Arthur-Gervais.pdf

Data integrity - World Economic Forum, Blockchain Toolkit, Data Integrity: https://widgets.weforum.org/blockchain-toolkit/data-integrity/

TradeLens - TradeLens architecture (IBM Blockchain Platform on Hyperledger Fabric), Port de Barcelona PierNext: https://piernext.portdebarcelona.cat/en/technology/tradelens-the-blockchain-platform-for-maritime-logistics - Maersk press release on TradeLens discontinuation, 29 Nov 2022: https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens - Supply Chain Dive coverage with Lars Jensen comment: https://www.supplychaindive.com/news/Maersk-IBM-shut-down-TradeLens/637580/

IBM Food Trust / Walmart mango pilot - Linux Foundation Decentralized Trust, Walmart case study: https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study

Everledger - Ledger Insights on Everledger collapse: https://www.ledgerinsights.com/everledger-bankruptcy-esg-blockchain-traceability/

GDPR - EDPB Guidelines 02/2025 on processing of personal data through blockchain technologies: https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

Alternative: standards and architecture - UN Transparency Protocol, Digital Traceability Events (UNECE): https://untp.unece.org/docs/next/specification/DigitalTraceabilityEvents/ - GS1, "GS1 Standards enabling the EU digital product passport": https://gs1.eu/wp-content/uploads/2024/12/GS1-Standards-Enabling-DPP.pdf

Regulation and direction of travel - EUDI ARF, Issue #278 (request to include DIDs in the ARF): https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/278 - Microsoft Entra Verified ID FAQ (did:ion deprecation): https://github.com/MicrosoftDocs/entra-docs/blob/main/docs/verified-id/verifiable-credentials-faq.md - CEN-CLC/JTC 24, EN 182xx series for the EU Digital Product Passport (published 27 May 2026): https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:3342699

Why the reflex persists - EU Blockchain Observatory & Forum, "Digital Product Passport, a Blockchain-based Perspective" (DG CNECT, 3 May 2024): https://blockchain-observatory.ec.europa.eu/publications/digital-product-passport-blockchain-based-perspective_en

IoT and sensor data - GS1 EPCIS 2.0 (EPC Information Services), including sensor data: https://www.gs1.org/standards/epcis - ISO/IEC 19987:2024 (EPCIS): https://www.iso.org/standard/85557.html

Money and currency instability - Chainalysis, 2025 Global Crypto Adoption Index (grassroots adoption in emerging markets, largely stablecoins for dollar access and inflation hedging): https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/

De Beers Tracr (high-value niche example) - Rapaport on GIA's 30% Tracr stake: https://rapaport.com/news/gia-acquires-30-stake-in-de-beers-tracr-platform/