

Blockchain in Agri-Food: Key Risks and How to Manage Them

Executive Summary

Blockchain technology promises tamper-proof traceability, trusted certifications, and more transparent supply chains for the agri-food sector. However, adopting it introduces real risks — not just technical ones, but strategic, regulatory, and financial. This report identifies seven major risk areas and offers practical guidance on how to address each.

The central takeaway is that blockchain is not something you simply “switch on.” It is a design and governance challenge. Every risk discussed here (from choosing the wrong platform to failing EU privacy rules) is manageable, provided it is addressed upfront rather than patched later. Two principles apply across the board. First, blockchain should be one piece of a larger trust system, not the whole system. Keeping your business processes, identity management, and data governance independent from the blockchain itself is the best insurance against long-term problems. Second, ongoing costs are consistently underestimated: running nodes, managing security keys, maintaining automated contracts, upgrading cryptography, and coordinating between consortium partners are all recurring expenses that need sustainable funding, not just startup budgets.

The report is ordered from the most immediately practical concerns (choosing a platform, connecting to existing systems) through to longer-horizon issues (the threat that future quantum computers may pose to today’s encryption).

1. Introduction

The agri-food sector is different from banking or finance, where blockchain has been tested more extensively. Food supply chains involve a wide range of participants (from small farms and cooperatives to logistics companies, supermarkets, and government inspectors) often with limited IT resources and connectivity. Margins are thin, and any technology adoption must justify itself in operational savings or regulatory compliance. This report looks at the specific risks that arise when introducing blockchain into this environment and suggests ways to manage them from both a technology and a business standpoint.

2. Risk Areas

2.1 Choosing the Wrong Platform (Vendor Lock-In)

What can go wrong: The blockchain market is crowded and fragmented. Some platforms are backed by large vendors, others by open-source communities, and others by niche startups. If a consortium builds its entire traceability system on a platform that later loses support (as happened with IBM Food Trust) the investment is largely stranded. Moving data and logic from one blockchain to another is far harder than switching between conventional databases.

What to do about it:

- **Build on open standards, not on a specific platform.** Use widely recognised data formats (such as GS1 EPCIS for supply chain events) and identity standards (such as W3C Verifiable Credentials) as the foundation. The blockchain then becomes a replaceable storage and validation layer underneath, rather than the layer everything depends on.
- **Back up critical records on more than one network.** For the most important data (export certifications, origin guarantees) it is inexpensive to record a cryptographic fingerprint on a second, independent blockchain as a safety net.
- **Write exit clauses into consortium agreements.** From day one, define what happens if the platform needs to change: who owns the data, in what format it can be exported, and what triggers a migration decision.
- **Why it matters for the business:** A consortium that is locked into a single vendor has limited negotiating power, cannot easily bring in public-sector partners, and may not meet the openness requirements of EU funding programmes like Horizon Europe.

2.2 Connecting Blockchain to Existing Business Systems

What can go wrong: Farms, logistics companies, and retailers already run on established business software, like ERP systems, warehouse management platforms, regulatory reporting tools. If the blockchain project requires people to re-enter data manually or needs expensive custom integrations for every partner, it will fail when moving from pilot to full-scale deployment.

What to do about it:

- **Use standardised middleware.** Integration platforms like IDSA Connectors act as translators between existing business systems and the blockchain. They handle data format conversion, access control, and usage policies in a standardised way, avoiding the need to build custom bridges for each partner.
- **Let the blockchain record only what it needs to.** Not every piece of supply chain data belongs on the blockchain. Design the system so that the blockchain captures a verified subset of events (e.g., “batch X passed inspection at facility Y”) while the full operational data stays in conventional systems.
- **Provide conventional access points.** Make blockchain-verified data available through standard web APIs that existing systems already know how to use. Do not expect a 20-year-old ERP system to talk to a blockchain directly.
- **Why it matters for the business:** Integration typically accounts for 40–60% of the total cost of blockchain projects in agri-food. Underestimating this is the most common reason pilots never become real products. Budgets must include connector development, data mapping, and the ongoing work of keeping formats aligned as systems evolve.

2.3 Privacy Regulation and the “Cannot Delete” Problem

What can go wrong: Blockchain’s core promise that records cannot be altered or deleted directly clashes with the EU’s General Data Protection Regulation (GDPR), which gives individuals the right to have their personal data erased. In agri-food traceability, personal data can easily end up on the chain: farmer names, farm GPS coordinates, inspector identities. EU data protection authorities have begun to take the position that storing personal data on an immutable blockchain is non-compliant by design.

What to do about it:

- **Never put personal data directly on the blockchain.** This is not optional. On-chain records should contain only anonymised references and cryptographic fingerprints. The link between an anonymous reference and a real person should exist only in a separate, conventional database where deletion is technically straightforward.
- **Use revocable digital credentials.** If a person’s identity is linked to a blockchain record through a digital credential, that credential can be revoked, effectively “forgetting” the person even though the blockchain record remains. The record becomes meaningless without the credential to interpret it.
- **Separate data catalogues from the blockchain.** Use EU-standard metadata catalogues (DCAT-AP) to describe what data exists, who can access it, and how long it should be kept. This governance layer lives outside the blockchain and can be updated or deleted as needed.
- **Why it matters for the business:** GDPR non-compliance is a deal-breaker for any EU-based consortium. Fines can reach 4% of annual global turnover. In a consortium, determining who is legally responsible for the data is already complex; adding an immutable blockchain without a clear deletion strategy makes the legal exposure unmanageable.

2.4 Handling Real-World Data Volumes

What can go wrong: A pilot with a handful of farms and a few thousand transactions per month is very different from a production system processing millions of IoT sensor readings during harvest season. Blockchains that performed well in testing may slow down or become prohibitively expensive under real-world loads, especially when automated rules (smart contracts) run complex validation checks on every transaction.

What to do about it:

- **Do the heavy computation off-chain.** Run complex checks (e.g., temperature monitoring, geofence verification, quality scoring) in conventional systems or at the network edge. Record only the final result and a tamper-proof fingerprint on the blockchain. This can reduce blockchain workload by 80–95% while keeping the audit trail intact.
- **Not everything needs the same level of guarantee.** A batch-level certification (“this shipment of olive oil is organic”) needs the strongest possible blockchain

guarantee. An individual sensor reading (“temperature was 4°C at 14:32”) can be bundled and summarised periodically. Design accordingly.

- **Match the security level to the trust relationship.** Many agri-food partners already have contractual relationships and a degree of mutual trust. The blockchain does not need to protect against every possible form of cheating for every transaction: only for the trust boundaries that matter most.
- **Why it matters for the business:** Over-engineering the system for maximum throughput and security at every level inflates infrastructure costs unnecessarily. The goal is to invest in blockchain guarantees where they add real value and use cheaper conventional approaches everywhere else.

2.5 Automated Contracts: Bugs and Upgrades

What can go wrong: Smart contracts (the automated rules that execute on a blockchain) can encode important business logic: releasing payment when a delivery is confirmed, flagging a supplier when temperature limits are breached, or issuing a certification. If these contracts contain bugs, they can be exploited to create fraudulent certifications, trigger incorrect payments, or disrupt operations. Unlike a bug in a website, a bug in a deployed smart contract can be very difficult or impossible to fix after the fact.

What to do about it:

- **Invest heavily in testing for certification logic.** Any smart contract that touches regulatory compliance (e.g., organic certification, geographical indication, phytosanitary clearance) should undergo the most rigorous testing available, including mathematical proof of correctness where feasible. The cost is justified by the consequences of failure.
- **Build in upgrade mechanisms with governance controls.** Smart contracts should be designed to be upgradeable, but only through a controlled process that requires approval from multiple consortium members. No single party should be able to change certification logic unilaterally.
- **Keep humans in the loop for high-stakes decisions.** Do not allow smart contracts to automatically execute irreversible, high-consequence actions (such as revoking a supplier’s certified status). Instead, have the contract flag the issue and route it to a human decision-maker.
- **Why it matters for the business:** A single exploited vulnerability in a certification contract could lead to product recalls, regulatory sanctions, and reputational damage across the entire consortium. The potential downside far outweighs the cost of thorough auditing.

2.6 Managing Keys and Digital Identities

What can go wrong: Every participant in a blockchain network holds a cryptographic key. This is essentially a digital signature that proves their identity and authorises their transactions. If a key is lost, that participant can no longer interact with the network. If a key is stolen, an attacker can sign fraudulent transactions that appear legitimate. In agri-food consortia, participants range from multinationals with dedicated IT security teams to

smallholder cooperatives using basic smartphones. The weakest link defines the consortium's security.

What to do about it:

- **Tailor key security to the participant's role and capabilities.** Certifying authorities and large retailers should use dedicated hardware security devices. Logistics providers can use the secure enclaves built into modern business phones and tablets. Smallholders may need a managed key service with social recovery mechanisms (similar to how you might recover a bank account through identity verification).
- **Separate identity from any single key.** Use decentralised identity standards (W3C DID) that allow a participant's keys to be rotated or replaced without losing their identity on the network. If a key is compromised, the identity survives.
- **Require multiple approvals for critical actions.** For operations that create high-value records (e.g., product batch certifications, export clearances), require digital signatures from multiple authorised parties rather than a single individual.
- **Why it matters for the business:** Key management failures are invisible until they become catastrophic. The cost of proper key governance is a recurring operational expense that must be budgeted explicitly and permanently, not treated as a one-time setup task.

2.7 Future-Proofing Against Quantum Computing

What can go wrong: All current blockchain platforms use encryption methods that will eventually be breakable by sufficiently powerful quantum computers. While such computers do not yet exist at the required scale, the threat is particularly relevant for agri-food traceability because the records need to remain trustworthy for decades. A certification of origin for a PDO product, for example, may need to be verifiable 20 years from now. An attacker could copy encrypted data today and decrypt it years later when quantum computers become available, a strategy known as "harvest now, decrypt later." If that happens, the entire integrity guarantee of the blockchain becomes worthless retroactively.

What to do about it:

- **Design the system so that encryption can be swapped out.** The most important decision is to ensure that the cryptographic methods used by the blockchain are not hardwired. The system should be built with a pluggable encryption layer, so that when quantum-safe algorithms become mandatory, they can be adopted without rebuilding the platform from scratch. Some blockchain platforms (such as Hyperledger Fabric) already support this; others (such as Ethereum-based systems) require workarounds.
- **Start adding quantum-safe protection in parallel.** International standards bodies (NIST in the US, ETSI in Europe) have recently finalised the first generation of quantum-safe encryption algorithms. These can be deployed alongside existing

encryption during a transition period, so that records are protected by both methods simultaneously.

- **Use interim measures for long-lived records.** Even before a full transition, critical records can be given extra protection by recording quantum-resistant cryptographic fingerprints on a dedicated notarisation layer. This provides an insurance policy without requiring immediate changes to the main blockchain.
- **Why it matters for the business:** The cost of quantum-proofing is an upfront investment, but the alternative (i.e., a retroactive breach that invalidates years of certified traceability data) would be existential for any consortium whose value proposition rests on trust. EU regulations (eIDAS 2.0, NIS2) are already beginning to reference quantum readiness, so early adoption also provides a regulatory compliance advantage.

3. Cross-Cutting Themes

3.1 Keeping Up with EU Regulation

The European regulatory landscape is moving fast and in a direction that both encourages and constrains blockchain use. The Data Act requires that smart contracts can be terminated or paused. The eIDAS 2.0 regulation defines how electronic attestations must be managed. The Digital Product Passport regulation will require verifiable, long-lived provenance records. Systems designed today must be compatible with these evolving frameworks. This reinforces the case for standards-based, upgradeable, privacy-compliant architectures.

3.2 Understanding the True Cost

The most dangerous business risk is not any single technical failure but the tendency to underestimate ongoing costs. Running blockchain nodes, managing cryptographic keys, maintaining smart contracts, upgrading encryption, keeping integrations working, and coordinating governance across a consortium are all permanent, recurring expenses. Sustainable adoption requires funding models (e.g., membership fees, per-transaction levies, or public co-financing) that cover operations over the long term, not just the initial build.

Appendix — Glossary

Term	Meaning
Blockchain	A distributed digital ledger that records transactions across many computers so that records cannot be altered retroactively
Consortium	A group of organisations that jointly operate and govern a shared blockchain network
Cryptographic fingerprint (hash)	A fixed-size digital summary of a piece of data; any change to the data produces a completely different summary, making tampering detectable
DCAT-AP	A European standard for describing datasets in data catalogues, enabling discovery and governance
DID	Decentralised Identifier — a digital identity standard that does not depend on any single authority
Digital Product Passport (DPP)	An EU initiative requiring products to carry verifiable digital records of their origin, composition, and sustainability
eIDAS 2.0	The EU regulation governing electronic identification and trust services
EPCIS	A GS1 standard for capturing and sharing supply chain event data (“what, where, when, why”)
ERP	Enterprise Resource Planning — the core business software used by most companies for operations and accounting
GDPR	General Data Protection Regulation — the EU’s primary data privacy law
GS1	The international organisation that maintains supply chain standards including barcodes and data exchange formats
IDSA Connector	A standardised software component for secure, policy-controlled data exchange between organisations
IoT	Internet of Things — networked sensors and devices that collect data automatically
Key (cryptographic)	A digital secret used to sign transactions and prove identity on a blockchain
NIS2	The EU directive on network and information security for critical infrastructure
NIST	The US National Institute of Standards and Technology, which sets cryptographic standards adopted globally

Term	Meaning
PDO / PGI	Protected Designation of Origin / Protected Geographical Indication — EU quality certification schemes
PQC	Post-Quantum Cryptography — encryption methods designed to resist attacks by future quantum computers
Smart contract	A programme that runs automatically on a blockchain when predefined conditions are met
Verifiable Credential (VC)	A tamper-proof digital certificate that proves a claim (e.g., “this farm is organically certified”) without revealing unnecessary information
W3C	World Wide Web Consortium — the international body that develops web standards