How Blockchain Adds Trust to Full-Chain Traceability

Governments, industry and consumers are demanding full-chain traceability (FCT) in seafood supply chains. Required to ensure regulatory compliance, product quality and corporate responsibility—it also informs consumers about the seafood they and their families consume.

Blockchain is an extremely powerful technology that adds trust in full-chain traceability. It can ensure data is not altered as it moves between trading partners and different traceability systems while still protecting data confidentiality. But blockchain does not ensure data is valid. Trace Register's Full-Chain Traceability platform uses blockchain to both ensure data is not altered, and continuous monitoring and continuous auditing (CMCA) to assess whether data is valid.

Data volumes have increased exponentially in the seafood industry. The demand for data about seafood products has grown from a handful of key data elements (KDEs) to hundreds. Today a single container of seafood can come with hundreds—and even thousands—of pages of information.

New data standards, spearheaded by the Global Dialogue on Seafood Traceability (GDST), enable FCT software interoperability. Data standards for product definitions and supply chain entities (SCEs) that support the unique needs of the seafood industry are being established. Adoption of common standards such as GS1 and EDI is enabling secure interoperability between different FCT software systems.

This brings a host of new challenges for the seafood industry with demands for interoperable FCT software that *ensures data security, protects confidential data, and enables the sharing of trustworthy high-quality data.*

How can FCT systems accomplish this?

> Most FCT systems ensure that data received from suppliers cannot be modified and the users "trust" the FCT solution to maintain data security. However, as FCT systems become interoperable a new level of trust will be required. Downstream members must trust their FCT system, and also trust all FCT systems used by upstream suppliers.

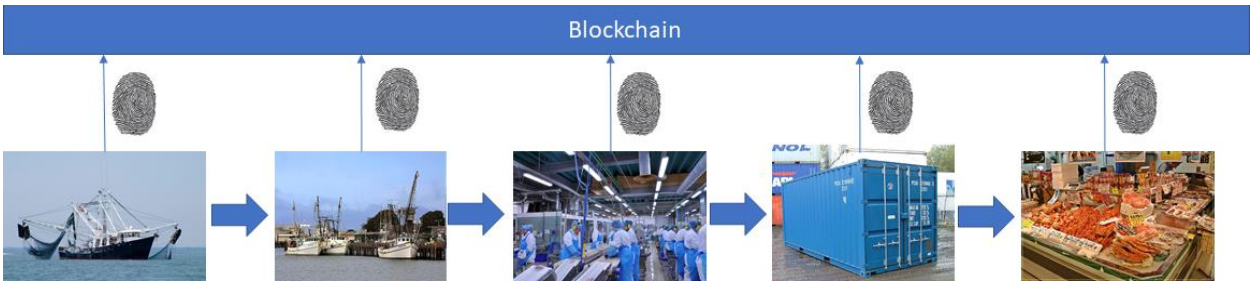
As data is captured and shared among different FCT systems how does a downstream supply chain member know if the data received upstream was changed by someone in the middle?

Proof is needed that the data entered by the vessel has *not* been modified. Each link in the supply-chain must trust that the receiving FCT system did not allow modification of "received data". As the number of parties in the supply chain increase, the number of "trusted parties" grows rapidly.

Blockchain is the solution to effectively solve this "trust" problem.

With blockchain, each party registers a fingerprint of their data on the blockchain. As downstream supply chain members receive the upstream data, they can quickly check the blockchain and confirm the received data has a valid fingerprint and be confident they have received untampered data.

- Data remains confidential, as the only registered data is the digital "fingerprint".
- Trust is moved from trusting everyone individually to trusting the "network".



However, while blockchains can help us "trust" that the data is not altered, it still cannot determine if the data is valid. For data validation, continuous monitoring and continuous auditing (CMCA) is the technology solution of choice.

A pioneer in full-chain traceability, Trace Register is also at the forefront of the blockchain revolution and brings the complete solution for both data trust and data validation by combining blockchain with CMCA.

Put the power of blockchain and CMCA to work with Trace Register and achieve data trust and data validation while keeping your proprietary information confidential.

Contact us today.