ORANGE TEAM PILOT

- Cryptowerk

"The Power of Many: Blockchain interoperability and portability for DSCSA Compliance"

Overview

The Orange Team Pilot proposes how a secure open source storage system housing encrypted and non-encrypted data can be used in conjunction with blockchain and other distributed ledger technologies to meet the data exchange requirements of both the Drug Supply Chain Security Act (DSCSA) and the industry at large.

This open-source, blockchain-validated solution is focused on interoperability and scalability in heterogeneous trading partner environments. It is designed to allow partners to securely store, validate, and exchange product tracing information and is intended to be complimentary to existing track & trace solutions. Additionally, it optionally leverages the superior security of public blockchains at scale for data integrity validation.

Team's vision

Today, the pharmaceutical industry leverages a variety of different serialization and supply chain providers to track and trace their products. It is this team's position that the industry will prefer to leverage existing heterogeneous solutions rather than agree upon one single solution for the industry.

Additionally, the team believes that no one company should hold the trust of the entire community and therefore proposes an open-source framework – validated by one or more blockchains of choice – to cryptographically store and share data.

Target audience

The presentation is designed for the CXO across the entire value chain – from manufacturers to wholesalers to dispensers who – without the need to dramatically alter what the systems have in place today, seek to understand and explore the options for how distributed ledger technologies and other secure mechanisms can enhance the data storage and validation process.

DSCSA focus

This pilot demonstration provides a framework for:

- Establishing an encrypted electronic data cloud-based warehouse between non-adjacent trading partners that is fed by existing data warehouses and immutably secured through distributed ledger technology
- Sharing required data and validating this data to be authentic
- Providing a permissioned mechanism for selective exposure of proprietary data upon request
- Establishing a framework for future industry discussions of implementation details

Pilot will demo:

- Interoperability
- Secure and selective data transfer
- Supply chain integrity

Technical aspects

This open-source solution allows for the storage and secure, selective access of DSCSA-required information and any other desired information by partners and regulators and consists of two key components:

1. One central, open source storage system, with a query engine
2. Many distributed open source Connectors for each partner

The central storage system manages secure connections and authenticated access for all partners, as well as query and (optional) payment facilities.