Supply Chain Provenance[1]

Smart contract based NFT Marketplaces with multi-sig

Gary Mawdsley CTO/CEO Lockular Limited

January 2024[2]

[1] Facilitated by Polkadot Parachains and NFT Marketplaces

[2] Updated April 2024 to reference Medicines supply chain example

This paper outlines the general concept of how an NFT Marketplace can be used to build supply chain provenance. In particular in talks of domain specific smart contracts, multi-sig and how to tie in real world assets[3].

[3] See the paper on coupling real and virtual worlds.

Introduction

Supply chain tracking is important across many domains. These include materials procurement in the defence sector, distribution of public examinations, assembly and distribution of drugs from manufacture, to wholssale, hospitals and patients to name a few.

This paper describes how Polkadot parachain-based NFT marketplaces offers a novel approach to tracking real-world supply chains by leveraging the interoperability and scalability of the Polkadot network.

But first: NFT stands for non-fungable token which implies it represents a unique instance of an object where one instance is distinguishable from another. This virtual token has to be associated with a real world property of one and only one instance of the real world object. For example for real world metals a "DNA" fingerprint can be obtained for an item. Two apparently identical metal items (e.g. two Apple laptop of identical model) will have a different "DNA" signature. As far as metals are concerned this is the representation of the unique grain structure of a metal or the specific distribution of impurities in a polymer.

Mapping a real world object instance onto an NFT is known as minting. Once mapped the buy, sell, transfer facilities of an NFT marketplace can be exploited to track the workflow of a supply chain. This takes place under the watchful eye of a domain specific smart contract where the transaction is authorised by all parties involved

In gerneral terms here's how Polkadot based NFT Marketplaces can be utilised for supply chain management:

- Interoperability Across Chains: Polkadot's architecture allows different blockchains (parachains) to communicate and share information seamlessly. This interoperability is crucial for supply chain management as more and more processes are onboarded, as it enables the integration of various stakeholders' systems onto a unified platform. For instance, manufacturers, logistics providers,

and retailers can operate on different parachains but still exchange data effortlessly, ensuring transparency and real-time tracking.

- NFTs for Unique Identification: Non-Fungible Tokens (NFTs) can represent unique physical assets in the supply chain, from raw materials to finished products. Each NFT can store essential data about the asset it represents, such as origin, production date, quality certifications, and journey through the supply chain. This unique identification helps in preventing counterfeits and ensuring the authenticity of the products.
- Smart Contracts for Automation: Smart contracts on Polkadot parachains can automate various supply chain processes, such as payments, certifications, and compliance checks. For example, a smart contract could automatically release payment to a supplier once the goods are verified and received by a smart contract-controlled NFT, reducing the need for manual intervention and speeding up transactions.
- Enhanced Security and Scalability: Polkadot's shared security model ensures that all parachains benefit from the collective security of the network. This model, combined with the scalability offered by parachains (each optimised for specific use cases), makes it an ideal platform for managing complex supply chains that require high levels of security and the ability to handle large volumes of transactions.
- Real-World Asset Integration: Integrating real-world assets with a digital representation (NFTs) requires a reliable way to verify the physical asset's status and update its digital counterpart accordingly. This can be achieved through IoT (Internet of Things) devices that monitor and relay information about the physical assets to the blockchain, ensuring that the NFTs accurately reflect the real-world state of the assets. Lockular uses the technique to track carbon saving in an estate of 600 industrial boilers.
- Decentralised and Transparent Tracking: The decentralised nature of blockchain ensures that no single entity has control over the entire supply chain data, promoting transparency and trust among all participants. Every transaction and movement of goods can be tracked on the blockchain, providing an immutable record that can be audited by authorised parties, including regulators and consumers.

Polkadot parachain-based NFT marketplaces represent a powerful tool for enhancing the transparency, efficiency, and security of supply chain management. By leveraging the unique features of Polkadot

and NFTs, stakeholders in the supply chain can achieve a level of interoperability and automation that was previously difficult to attain, paving the way for more resilient and responsive supply networks.

Smart Contracts

Smart Contracts are code blocks that define the rules of workflow to the Marketplace for a given domain. Smart contracts used to control NFT marketplaces for tracking real-world supply chains will differ significantly across domains due to the unique requirements, regulations, and challenges inherent to each sector. Here's a couple of examples that show how smart contracts might vary between the domains of metals and alloy manufacture compared to the manufacture of medicines:

Metals and Alloy Manufacture

- Quality Verification: Smart contracts in metals and alloy manufacture would include specific conditions related to the quality and specifications of the materials, such as composition, grade, and physical properties. These conditions must be met and verified, possibly through linked IoT devices or certified laboratory results, before transactions can proceed.
- Source and Sustainability Tracking: Given the increasing importance of sustainable and responsible sourcing in the metals industry, smart contracts can be used to encode the origin of materials and ensure that they comply with environmental and ethical standards.
- Batch Tracking and Segregation: In metals and alloy manufacturing, it's crucial to track specific batches of materials to ensure they meet the required standards for particular applications. Smart contracts help automate the segregation and tracking of these batches throughout the supply chain.

Manufacture of Medicines

- Regulatory Compliance: The pharmaceutical industry is highly regulated. Smart contracts in this domain would need to incorporate mechanisms for ensuring and proving compliance with various regulatory requirements at every step of the supply chain.
- Temperature and Handling Conditions: Medicines often require controlled temperatures and specific handling conditions to maintain their efficacy. Smart contracts could be programmed to verify

these conditions have been maintained throughout the supply chain, using data from IoT sensors.

- Counterfeit Prevention and Recall Management: Given the critical importance of authenticity in pharmaceuticals, smart contracts would include features for anti-counterfeiting and efficient recall management. They would ensure that only verified entities are part of the supply chain and enable rapid action if a batch needs to be recalled.

Commonalities and Differences

While there are domain-specific requirements, there will be some common features across different industries:

- Transaction Automation: Automating payments and transfers upon meeting predefined conditions.
- Transparency and Traceability: Providing a transparent and immutable record of the supply chain journey.
- Stakeholder Verification: Ensuring that all parties involved in the supply chain are verified and authorised to participate.

The primary contract definition differences arise from the specific challenges and regulatory requirements of each domain.

Ensuring Authorised Parties are Verified and Authorised

Ensuring that all parties involved in the supply chain are verified and authorised to participate is crucial for maintaining the integrity and security of the supply chain. Multi-signature (multi-sig) technology plays a significant role in achieving this, especially in the context of blockchain-based supply chain management and smart contracts.

Multi-Sig

Multi-sig refers to a digital signature scheme which requires two or more parties to sign off on a transaction before it can be executed. In the context of blockchain and smart contracts, this means that a transaction (such as transferring an NFT representing a physical asset in the supply chain) would require the approval of multiple stakeholders before it can proceed.

Multi-Sig provides the following features:

- Enhanced Security: By requiring multiple signatures, multi-sig ensures that no single party can unilaterally make changes or complete transactions. This reduces the risk of fraud and unauthorised

actions, as collusion would be required among multiple verified parties to bypass the system.

- Verification of Parties: Multi-sig can be used as a mechanism to ensure that all parties involved in a transaction are verified and authorised. Before a party can be part of the multi-sig arrangement, they must be vetted and approved, adding an additional layer of trust to the transaction.
- Dispute Resolution and Compliance: In cases where disputes arise, or compliance needs to be verified, the multi-sig requirement ensures that there is a transparent and auditable trail of approvals. This can be crucial for resolving disputes and demonstrating compliance with regulatory requirements.
- Decentralised Trust: Multi-sig decentralises trust among multiple parties, reducing dependency on a single entity for the security and integrity of transactions. This is particularly important in supply chain management, where multiple independent entities must collaborate and trust each other.

Implementation in Supply Chains

In a blockchain-based supply chain, smart contracts should be designed to require multi-sig for critical actions, such as updating the status of an asset, transferring ownership of an NFT, or releasing funds. The parties involved in these signatures must include the stakeholders, i.e. manufacturers, logistics providers, quality assurance entities, and possibly even regulatory bodies, depending on the requirements of the domain.

For example, a smart contract governing the transfer of an NFT representing a batch of pharmaceuticals might require signatures from the manufacturer, the logistics provider, and a regulatory compliance officer. Only when all parties have reviewed and approved the transaction (e.g., confirming that regulatory and handling requirements have been met) can the transfer proceed.

Multi-sig is employed in Lockular NFT Marketplaces and provides a powerful tool for ensuring that all parties involved in a supply chain are verified and authorised to participate. By leveraging multi-sig in smart contracts, blockchain-based supply chain management systems exhibit elevated security, trust, and compliance, making them more resilient and reliable.

References