SIMBA®

Reducing Supply Chain Fraud Through Assured Digital Identity for Physical Devices

Today's global economy faces significant challenges resulting from counterfeit items entering the supply chain. This exposes manufacturers and product users to various risks, including components failing to meet quality expectations due to inferior production lines, which has widespread economic, safety and security implications.

Table of Contents

1 Introduction

Today's global economy faces significant challenges resulting from counterfeit items entering the supply chain. This exposes manufacturers and product users to various risks, including components failing to meet quality expectations due to inferior production lines, which has widespread economic, safety and security implications. The Organisation for Economic Co-operation and Development (OECD) recently reported that counterfeiting represented $461B of world trade, with more than 500,000 customs seizures. For the DoD, a resilient, redundant and secure supply chain is required to ensure the development and sustainment of capabilities critical to national security, and to ensure the appropriate level of safety is maintained for the warfighter. Counterfeit parts have become a significant threat to the defense supply chain, which affects every component, from off-the-shelf assemblies, to microchips and large military platform assemblies. Eliminating counterfeits would help the DoD reduce risk and cost while significantly improving system performance, yet maintaining the integrity of parts across the supply chain remains a troublesome issue.

In the commercial sector, this issue is widespread also. As a recent example, in 2019, farmers from the Big Island's Kona district sued more than 20 companies in February 2019 after a lab test reportedly confirmed long-held suspicions that beans being marketed as Kona coffee weren't actually from the iconic region. The lawsuit claimed that 2.7 million pounds of authentic Kona coffee beans are grown each year and yet more than 20 million pounds of coffee labeled Kona are sold. A total of more than 27 Million dollars was settled in these lawsuits, which outline the severity of the issue.

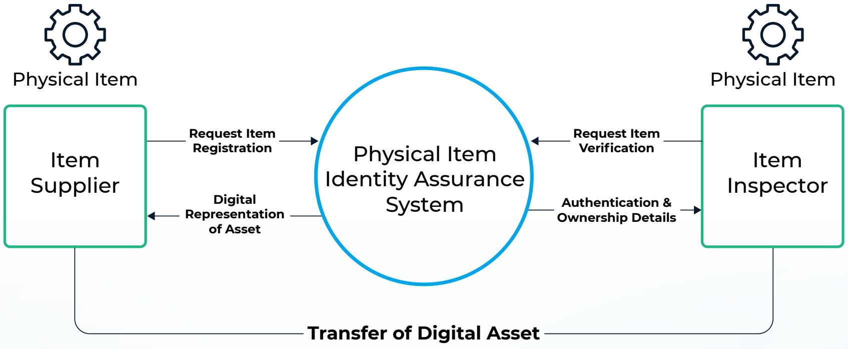
One approach to reducing the prevalence of counterfeit items is to be able to positively identify the physical characteristics of genuine parts, and then reliably verify the presence of these items through the supply chain. As a result, any item that can not be positively identified and recognised as genuine can be treated as suspicious, and made subject to further investigation. This solution can provide all parties involved with a supply chain with irrevocable proof that the components, parts or products they are dependent on are genuine, and can be relied upon to provide high quality, safe and secure products. Furthermore, the solution can provide proof of ownership of items, and a demonstrable trail of past ownership, to provide items with provenance. To take full advantage of such a solution, participants need to be able to trust the integrity of underlying data used to make assertions about the identity and ownership of an item; that is, to maintain integrity of the digital twin binding for anti-counterfeiting purposes. This data needs to be tamperproof, so that bad actors are unable to inject data about counterfeit parts into the system, passing them off as genuine, or make unauthorized changes to ownership records. Furthermore, the data needs to be traceable, and irrefutably linked to the physical part, removing any doubt about the provenance of the item.

1.1 A Blockchain Approach

A decentralized blockchain technology approach, which can provide an unhackable binding between the physical to the digital, is a realistic and robust solution to the counterfeit problem . The solution uses the widely adopted ERC-721 non-fungible token (NFT) standard to provide a digital record, or receipt, for a physical part. NFT's have properties that enable them to be used to uniquely represent assets, which provides a robust means of representing any unique item in the digital world, and the associated standards express how data can be represented and assets transferred between parties, providing interoperability. As such, NFTs provide a solid framework for representing unique items in the digital world.

The essence of this approach involves taking a digital fingerprint that uniquely maps to the physical item, then registering a deterministic representation of this fingerprint into the NFT. Now, since the NFT incorporates the unique physical characteristics and an NFT is digitally signed by the user that created it, this solution effectively provides a means of digitally signing physical parts. So, in the same way that a digital signature can guarantee that data has not been changed, the signed digital fingerprint of the physical part, housed within an NFT, proves that the physical part has not changed during the transition between a sender and receiver. This approach is capable of securing a supply chain and eliminating counterfeiting altogether.

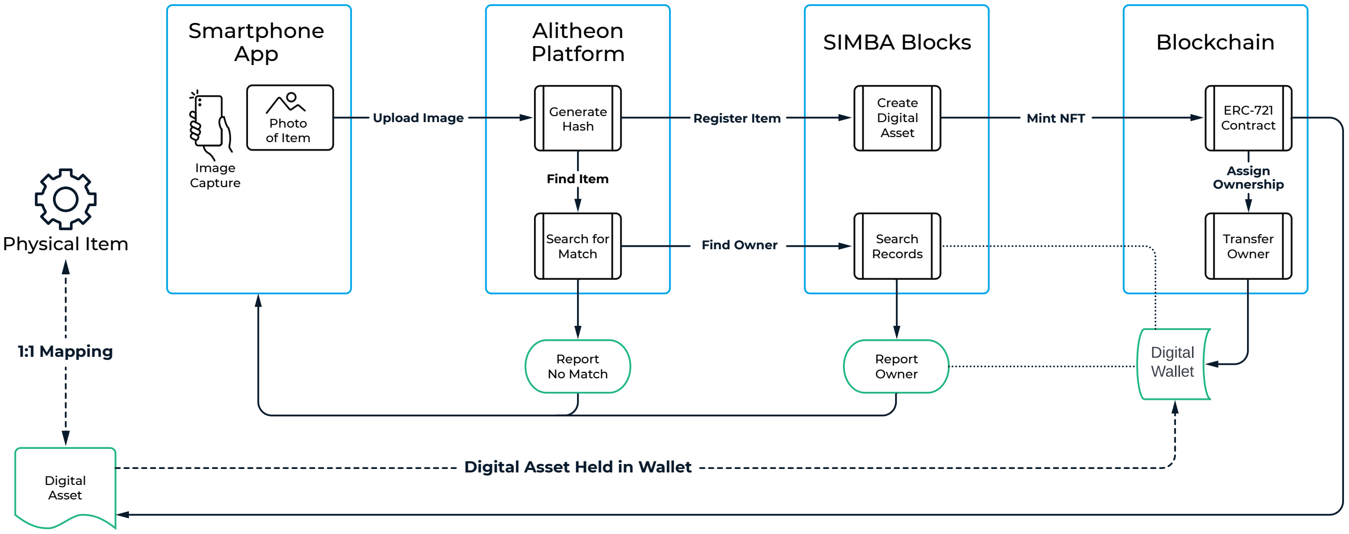
The architecture described can be used to provide assurance, provenance, and proof of ownership of items using secure, digital fingerprints of genuine physical components. These digital fingerprints provide the basis for delivering trust and integrity across the supply chain by capturing an evidence trail that demonstrates that items are authentic, and legitimately owned. The context diagram below shows how the solution would provide an assurance layer between a supplier of an item and an inspector, or prospective buyer of the item.


Physical Item
Item Supplier
Request Item Registration
Digital Representation of Asset
Physical Item Identity Assurance System
Request Item Verification
Authentication & Ownership Details
Physical Item
Item Inspector
Transfer of Digital Asset

Context Diagram

2 Architecture

The following diagram shows the architecture and process flow of a solution that identifies and registers a physical item, providing a digital representation of the asset that can be used for track and trace in a supply chain through mechanisms that demonstrate authenticity and prove the legitimacy of ownership.



The architecture includes the following components:

2.1 Smartphone App

The Alitheon app uses the smartphone's camera to take a digital photograph of the physical item of interest, or a predefined region of the item. The app sends the photo to Alitheon's service, which generates a unique identifier (called a featureprint) for the item based on analysis of the image. The app allows new items to be registered or starts a process of verifying that an item being inspected matches an original authentic item previously registered in the system.

2.2 Alitheon Platform

The digital photo from the smartphone app is uploaded to Alitheon's platform, which uses optical AI techniques to convert the minute surface details of a physical item into a mathematical featureprint that uniquely represents the item, acting as a digital fingerprint and the basis for identifying the item. The Alitheon platform provides registration of newly presented items, and subsequently determines whether a presented item matches a previously registered item during verification checks.

2.3 SIMBA Blocks

SIMBA's Blocks platform provides interfaces between the solution logic and the underlying blockchain NFT smart contract, in the form of REST APIs and SDKs in popular programming languages. This accessible abstraction layer simplifies the development of blockchain-based applications and solutions, and supports subsequent migration of the solution to alternative blockchains. A benefit of this approach is that it provides appropriate levels of scalability during proof-of-concept, and in production. The SIMBA platform provides integration with leading cloud providers, and enterprise security models, bringing proven Web2 practices to Web3.

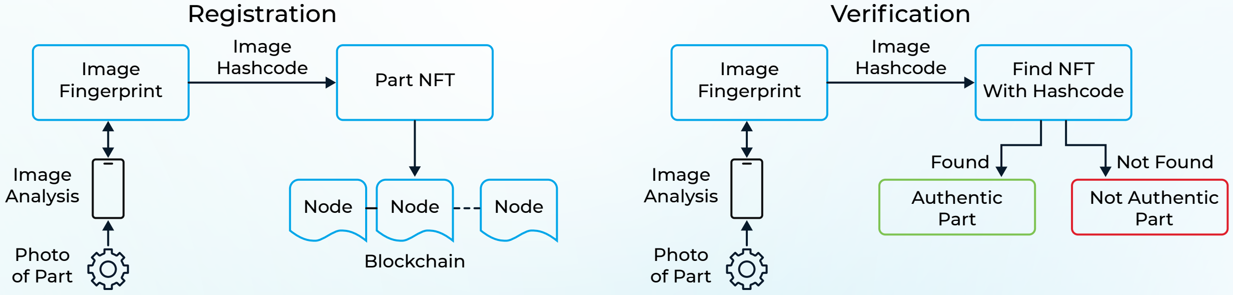
2.4 Blockchain Smart Contracts

The business logic of the solution is contained in smart contracts, which write assets and transactions onto a blockchain. This provides an immutable record of written data, providing a single source of truth about items registered in the system. Here, the unique identifier for an item is written to the blockchain by a trusted party, in a transaction that is ratified by a digital signature. This provides a mechanism that records the unique identifier of the item when it is registered, and is used to validate the item when it is inspected. Furthermore, by adopting established standards for blockchain data storage and transfer, changes in ownership of the physical item can be replicated in the digital world, providing a digital receipt for any transactions involving the item.

2.5 Digital Wallet

Digital wallets are used to trace and prove ownership of physical assets in the digital sphere, through an irrefutable mapping of the physical item to a digital counterpart held in an NFT. A digital wallet is controlled by a private key - this acts as a secure password that enables the wallet's owner to demonstrate that they have control of the wallet. The digital asset that represents the physical item is held in a digital wallet, and the controller of the wallet is able to use a digital signature to prove that they have the key to the wallet. If the holder of the physical item can demonstrate that they have ownership of the digital wallet that contains the digital asset representation, then it can be taken that their ownership is legitimate. When the physical item is sold or transferred, the digital asset should be digitally signed and transferred to a wallet that belongs to the new holder of the item, maintaining the provenance trail.

Further details on the role and interactions between these components is given below. The following diagram shows the workflow of registration and subsequent verification of a physical item.



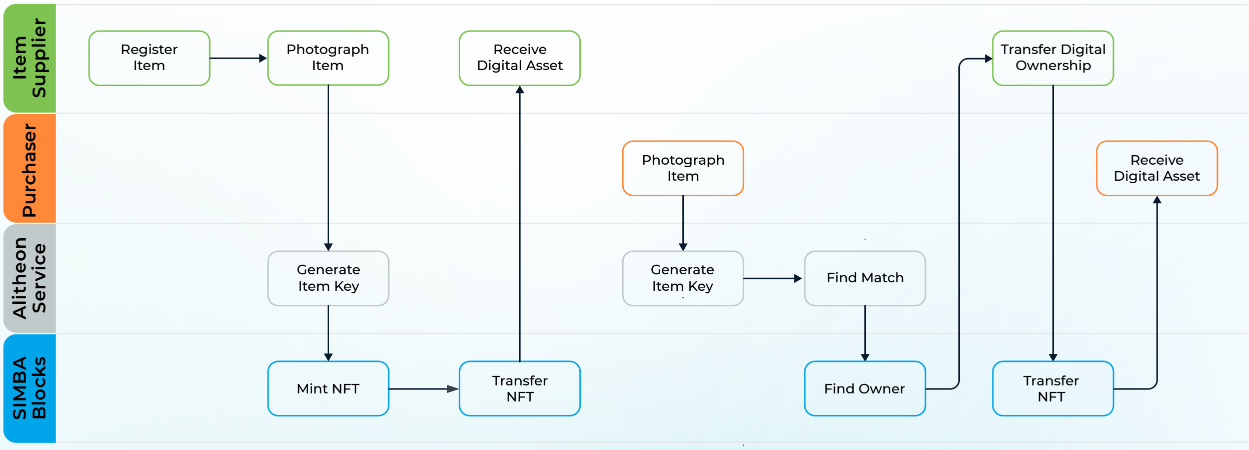
Registration and Verification of Physical Items

This process can be used to register a physical item, creating its digital counterpart and assigning it to the owner of the item. Subsequently, a presented item can be checked to verify that it is the original item, and that its ownership matches that of the digital counterpart. Changes in ownership of the physical item can be replicated in the digital world by transferring ownership of the digital asset. Using an NFT as the format of the digital representation of the item provides traceable records of transfers of ownership of the item, using widely adopted technologies. The steps for such a workflow are summarized as follows:

1. The item's supplier uses an app to take a photograph of the item, and registers the image with the Alitheon service. The service creates a unique fingerprint, the hashcode, for the image.
2. A request is sent to SIMBA's platform for an NFT to be minted. The request contains a name, description and the hashcode for the item. SIMBA mints the NFT on the blockchain, and transfers ownership of the NFT to a digital wallet controlled by the supplier. Ownership of both the physical item and the digital representation are now with the supplier.
3. If the item is to be sold, a prospective buyer takes a photo of the item and requests authentication of the image from the Alitheon service. The service generates a hashcode for the uploaded image, and then tries to locate the image among its archives of registered items. If there is a match, the item is authenticated - otherwise it doesn't match any registered item.
4. If the item is authentic, the solution queries SIMBA Chain to find the digital representation of the item. This would be the NFT that contains the matching hash. The buyer verifies that the NFT is held in a digital wallet controlled by the supplier. This provides assurance that the party trying to sell the item is the legitimate owner.
5. Once all checks are completed satisfactorily, the supplier sends a transfer request to SIMBA Chain to move the NFT into the buyer's wallet, and simultaneously transfers the physical item. This provides the item's new owner with a digital receipt for the item, and maintains the provenance trail of ownership of the item.

As a result, the integrity of the physical item has been verified, and the change in ownership replicated in the digital sphere, through a transfer of the NFT representing the device to a wallet owned by the buyer. As all transactions are conducted on a blockchain, an immutable trail is written, providing full traceability of the ownership of the item.

The steps of this process are illustrated as follows:



Registration and Transfer of Digital Assets

3 Analysis

The architecture is based upon a novel approach to component identification, developed by SIMBA's partner Alitheon. The process uses a unique algorithm to analyze digital images of physical items, which finds the unique digital fingerprint for any item. This enables a true, irrefutable identity of each physical item to be determined, without any contact or alterations being made to the item. From gears and circuit boards, to watches and collectables, no two objects are exactly the same - even though they may have just come out of the same production line. As the fingerprint of the original, authentic, part and any other item is so different, it is impossible to fabricate a replacement part that can generate the same fingerprint as the original.

The process of binding a physical item to its digital representation is initiated from a photograph of the part. The Alitheon service uses this image to generate the unique digital featureprint for the item, which is converted, using a one-way deterministic function, into a hashcode. Once in receipt of the hashcode, a trusted party (eg. the item's manufacturer) sends a request to the SIMBA platform for an NFT to be created. The request contains a name for the item, a description and the physical item's hashcode. In response, the SIMBA platform calls a smart contract that mints a unique digital representation of the asset on a blockchain. Ownership of the digital asset is transferred to a digital wallet controlled by the trusted party, which provides an irrefutable link between ownership of the physical item and its digital counterpart.

Since the hashcode uniquely represents an individual physical part or component, the NFT in which it is embedded can uniquely represent the item in the digital domain. Once the item has this corresponding NFT-based digital representation, it can be checked for authenticity at any time and location, using a smartphone app. This verification of authenticity follows a similar process of generating a hashcode for the component under consideration, and comparing that with the hashcode "baked in" to the NFT representation of the genuine device. If they match, then interested parties can be assured that the device is genuine, otherwise it may be a counterfeit or replacement, and should be subject to further investigation.

Furthermore, ownership of the physical component or part can be transitioned between parties using an NFT transfer following standard, and widely adopted, ERC-721 methods. By transferring ownership of the NFT to digital wallets controlled by different participants in the supply chain, it can be tracked as it moves through the supply chain, recording both the transfer event and the legitimate custodian of the part. Every transaction is digitally signed by the transferring party, providing a trail of accountability.

3.1 Why Blockchain?

Blockchain technology is used to uphold a digital representation of a genuine physical item registered in the system. The use of a blockchain ensures that the original data registered and recorded for any item is fixed, and can never be changed. This essentially creates a secure, unhackable digital counterpart for each physical item. The link between the physical item and its digital counterpart is underpinned by encapsulating the unique digital fingerprint of the item into the tokenized digital representation using the standard ERC-721 NFT format.

The use of a blockchain brings a number of advantages:

- Embedding the unique hashcode into a blockchain-based representation of the asset provides the NFT with a direct mapping to the physical part, which can never be changed. This creates a digitally signed non-repudiable binding for a part in a supply chain, or other physical asset. On creation, ownership of each NFT is digitally transferred to the item's manufacturer, or a trusted custodian, using a digitally signed blockchain transaction, to provide resilient digital identification, traceability and accountability.
- By using an ERC-721 NFT format to carry the representation of the item, any transfer of ownership of the physical item can be replicated using the standardized transactions for transferring ownership of an NFT, in parallel with the physical transportation and delivery. This widely adopted functionality provides the means for unhackable and identifiable part traceability.
- Digital signatures are used to verify that the custodian of the physical item matches the ownership of the NFT. If it does, then the part is authentic and is demonstrably held by its legitimate owner. However, if the digital identity is not correctly matched then the part cannot be verified and may be deemed as not authentic. Further, if the part is identified but the digital owner is incorrect, then this can indicate that ownership of the physical part has not been transferred legitimately.

In summary, the use of blockchain technology provides mechanisms for a trusted party to write data that cannot subsequently be changed, allowing others to put trust in the integrity of the digital identifier of the original item. Adoption of NFT standards brings additional benefits, as the solution can interface with the wider Web3 ecosystem and its tools to transfer and verify ownership of the item's digital counterpart.

Blockchain introduces undoubted benefits, but currently adoption and use of this nascent technology brings a number of challenges to solution teams. Typically, development is complex and tooling is rudimentary, requiring significant expertise to master, and to integrate securely with existing systems. There are a number of different blockchain models and platforms from which to choose, each suited to different business configurations and stages of project development and deployment. Teams face challenges in adopting the right solution, and maintaining that solution as their projects reach production scale. Furthermore, development in new blockchain technologies themselves is ongoing, and migration from one chain to another can introduce significant challenges at a later stage of a project lifecycle, potentially leading to lock-in with an obsolete blockchain.

3.2 Why SIMBA Chain?

Blockchain technology is used to uphold a digital representation of a genuine physical item registered in the system. The use of a blockchain ensures that the original data registered and recorded for any item is fixed, and can never be changed. This essentially creates a secure, unhackable digital counterpart for each physical item. The link between the physical item and its digital counterpart is underpinned by encapsulating the unique digital fingerprint of the item into the tokenized digital representation using the standard ERC-721 NFT format.

3.2.1 Provenance Tracking

SIMBA Chain provides an asset graph that stores data about each transaction on the blockchain. This asset graph is aware of standard smart contracts and their interfaces, which means that, in the case of an NFT, the asset graph stores NFT mint and transfer operations that incorporate the details of the sender and receiver wallets. Consequently, by using a single GraphQL query on an NFT asset, Blocks can retrieve the complete provenance of an NFT. For a supply chain scenario, that provenance would provide details of each step, or tier, in the supply chain transportation of that part during its lifetime, bringing full and secure transparency to the entire process.

3.2.2 Account and Digital Wallet Management

SIMBA's Blocks has been designed to work in enterprise settings, so it integrates with user authentication and authorization systems already in use. This hides complexity often associated with Web3 deployments, which can require users and administrators to manage and maintain cryptocurrency wallets as separate applications. With Blocks, the digital wallet is built into the platform, which means it ties into well established user on-boarding and management processes, and doesn't require new apps or administration of secure keys. An additional benefit of this is that any "gas fees" associated with blockchain transactions are taken care of by Blocks, not end users, which removes the need to manage cryptocurrency and authorize payments within business solutions.

3.2.3 APIs, SDK and Cloud Integration

Blocks provides a number of ways that developers can access and use blockchain smart contracts to extend their applications. From standards-based REST API interfaces that are dynamically generated from smart contracts methods, to software development kits in popular languages that interface into locally or cloud-hosted development solutions already in widespread use, Blocks provides tooling that enables teams to concentrate on their solution, not on learning new languages and design philosophies.

3.2.4 Flexibility, to avoid Lock-in

Blocks provides mediation between an application's business logic and the underlying blockchain platform. This means that the complexity of blockchain interaction is abstracted away from developers – and enables teams to pick and choose from a range of underlying blockchain platforms, each suited to particular situations, both public and consortium chains, for test and production. What's more, Blocks enables developers to change the blockchain they deploy their solution to as their business needs change - the complexity is taken away, and looked after by the Blocks platform.

3.3 What problems does it solve?

The architecture presented here provides a way to detect counterfeit items and products, which can prevent them entering the supply chain and help to reduce a range of serious risks introduced by poor quality or malicious replacements. The same approach can also be used to protect consumer to consumer transactions.

The architecture provides a digital representation of an item, which is intrinsically linked to the physical item by a digital fingerprint which is registered on an unhackable blockchain. The digital representation is able to provide proof of legitimate ownership of the physical item.

The use of digital signatures in the architecture provides traceable accountability, as parties must sign transactions and requests using a digital key that is unique to them. Any party that transfers the digital counterpart to another must provide a signature for the transaction to complete. This builds into an audit trail of all parties that have had ownership or custody of the item.

The architecture provides transparency and traceability of actions of all parties concerned with an item. This helps to reduce asymmetry of access to information and improve trust between participants in the ecosystem by maintaining a single, shared and trustworthy data source.

Building the solution on SIMBA Blocks provides the utility of blockchain without complexity, and enables the solution to integrate into enterprise environments using familiar development and devops methods and tools.

3.4 What are the advantages of the approach?

Instead of trying to spot counterfeits using processes that are prone to error, the solution is able to positively identify legitimate parts. This does not require any modification to the physical item, or the use of additional identifiers, such as QR codes, or NFC tags. Each item is identified by analysis of its own image. The solution is robust, and is able to correctly match on incomplete images, or when parts are dirty or damaged. This provides a digital fingerprint of the part which can be authenticated at any time, helping to eliminate counterfeit parts and products.

Use of a blockchain and digital signatures helps to make the system secure, as the data stored when an item is registered can’t be altered. This prevents bad actors from subsequently hacking a database to insert incorrect device fingerprints that match counterfeit items inserted into the supply chain. Digital signatures provide accountability on actions taken, so that any transfers or changes in ownership of items can be matched with expectations, and traced back for investigation.

In summary, a key to any track and trace solution is binding a physical item with its digital record. Currently, the technology to do that is an active tracking mechanism: bar code, QR code, embedded NFC tag, etc. All of those require implanting a device or marking, and something to read that implanted device/marking. And they all can be spoofed. This approach solves that by making it a passive read of the object, and underpinning data storage with an immutable blockchain record.

simbachain.com info@simbachain.com

SIMBA