UNIVERSITY OF TARTU
Institute of Computer Science
Software Engineering Curriculum

Antony Oroko Orenge

Blockchain-based Provenance Solution for Handcrafted Jewellery

Master’s Thesis (30 ECTS)

Supervisors:
Fredrik Payman Milani, PhD
Luciano Garcia Banuelos, PhD

Tartu 2018

Blockchain-based Provenance Solution for Handcrafted Jewellery

Abstract:

Handcrafted jewellery involves use of hand labour rather than manufacturing machinery. Unlike manufactured jewellery which is similarly crafted, cheap and easy to find, handcrafted jewellery tend to be uniquely crafted and fairly expensive, especially when it is attributed to a well known artisan or designer. The current information age has birthed a new era of conscious consumers who are willing to pay more for products with proven origins. Likewise, creators desire to be rightfully attributed and acknowledged for their work. However, the partial implementation of provenance by current solutions has encouraged opaque supply chains that hinder transparency and traceability. For this reason, there has been a rapid increase in counterfeit products, unprecedented economic loss, environmental degradation, health risks, increase in defamation cases, and broken trust. In this thesis, we review related provenance solutions using blockchain technology, identify key provenance features and implement a provenance solution for handcrafted jewellery on Ethereum blockchain. The output of this research can be used towards the development of provenance as a subject and its implementation in global supply chains.

Keywords:

Provenance, traceability, transparency, handcrafted, jewellery, artisans, blockchain, ethereum, smart contracts

CERCS: P170 - Computer science, numerical analysis, systems, control

Plokiahelapõhine lahendus käsitööehete päritolu jaoks

Abstrakt:

Käsitsi tehtud ehete valmistamiseks kasutatakse tootmismasinate asemel inimeste kätetööd. Kui masinate poolt tehtud ehted on samasugused, odavad ja kergesti kättesaadavad, siis käsitsi valmistatud ehted on ainulaadsed ja küllaltki kallid. Seda eriti siis, kui tegemist on tuntud käsitöölise või disaineriga. Käesolev tehnoloogiaajastu on tõstnud tarbijate teadlikkust ning inimesed on valmis rohkem maksma tõestatud päritoluga toodete eest. Samuti soovivad tootjad oma töö eest saada tunnustatud ja omada selle õigusi. Praegused lahendused on pärituolu osas poolikud ning see võimaldab tarneahelal olla läbipaistmatu ning seetõttu kõrvale hiilida läbipaistvusest ning jälgitavusest. Seetõttu on hüppeliselt kasvanud võltstoodangu arv, mis toob kaasa majandusliku ja keskkondliku kahju, terviseriskid, valdkonna halva maine ning rikutud usalduse. Käesolev dissertatsioon vaatleb ja selgitab plokiahela tehnoloogial põhinevaid lahendusi ja võimalusi taustakontrolli tegemiseks ning teostab Ethereumi plokiahelal põhineva lahenduse käsitööehete päritolu kontrolliks. Uurimuse tulemus aitab kaasa taustakontrollimehhanismide arengule ning aitab seda rakendada ülemaailmse tarneahela läbispaistvamaks muutmisel.

Võtmesõnad:

Päritolu, jälgitavus, läbipaistvus, käsitöö, ehted, käsitöölised, plokiahel, ethereum, nutilepingud

CERCS: P170 - Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Table of contents

1 Introduction

1.1 Motivation

Jewellery can be considered handcrafted if its production process mostly involved use of hand labour rather than manufacturing machinery. Handcrafted jewellery tend to be of more value, especially when handcrafted by a well known artisan, and meaningfully unique, unlike manufactured jewellery which is easy to find and cheap, but falls short of quality and artistry. The reason is that artisans who produce handcrafted jewellery are directly attributed to their work, thus they prefer to use ethically sourced materials with a high degree of quality. The craftsmanship employed on each piece is unique and this offers a special quality and variation from piece to piece. Each piece carries a distinct long story from a creative concept to a piece that connects the artisan to the consumer.

Currently, the opening up of economies, proliferation of internet usage and media revolution has resulted to a tech-savvy and conscious consumers who expect more and more transparency into the history of products they buy. This consumer awareness has encouraged jewellery manufacturers to develop brands that stand for quality and transparency. Furthermore, artisans in handcrafted jewellery have always desired to be rightfully attributed and recognized for their creativity and skilled labour. Therefore, there is a need to establish provenance for handcrafted jewellery supply chain so as to establish trust, and ensure transparency and traceability.

Provenance for a piece of handcrafted jewellery allows us to identify who is the creator, when, where, why and how it was created. Since provenance is an extrinsic value, it can only be shown to exist by valid documentation which needs to be corroborated beyond any reasonable doubt. Hence, we need a reliable, secure and trustworthy solution to establish provenance across the handcrafted jewellery supply chain so as to ensure transparency and traceability. The ISO 9000 2015 defines traceability as the “ability to trace the history, distribution, location, and application of products, parts, materials, and services” [1].

The common way by which consumers determine provenance of a product they buy is through manufacturers labels such as ‘Made in China’. However, such labels are vague and devoid of authentic and trustworthy information such as source of raw materials and manufacturing processes. Similarly, distributors find it difficult to determine the origins of a product since they rely on integrating with heterogenous enterprise systems to track and trace the origin and movement of products in the supply chain. This lack of provenance has led to opaque supply chains that encourage counterfeit trade, unfair pricing, unethical labor practices, environmental degradation, loss of revenue and a growing list of defamation cases.

This research proposes to design and implement a provenance solution for handcrafted jewellery using blockchain technology. The use of blockchain provides us with a cryptographically secured and trustless distributed ledger with an immutable nature. This ensures that provenance can be guaranteed across complex global supply chains. With trustworthy and authentic sources of provenance, transparency and traceability can be achieved and largely curtail the negative issues presented above.

1.2 Goal and Problem Statement

In this thesis, we present the key features required in designing a blockchain-based provenance solution and suggest a design pattern that can be re-used by interested parties in designing similar solutions. The goal of this research is to provide a reliable provenance solution that can guarantee transparency and traceability for the handcrafted jewellery global supply chain.

We define our research goals as follows:

1. What is the state of art of blockchain-based provenance solutions?
2. What are the key features in designing a blockchain-based provenance solution?
3. How to implement a provenance solution for handcrafted jewellery based on blockchain technology?

In addressing these questions, we review four related blockchain-based provenance solutions. We analyse each of one of them and extract key features that are required to design a provenance solution based on blockchain. Then we look into a specific case of handcrafted jewellery and draw from the existing use cases to create a novel solution that will be implemented on Ethereum blockchain network.

This paper is structured as follows:

Section 2 presents background information by describing the core technologies used in this paper. Section 3 analyzes related work from other provenance solutions based on blockchain technology. We conclude by discussing the key features in designing a blockchain-based provenance solution. Section 4 details the main contribution of this project, we start by describing the handcrafted jewellery business process and propose a proof of concept for our case study. Section 5 describes the implementation of our proof of concept and evaluates whether it answers our research question. Section 6 summarizes the answers to our research questions and provides additional information on how to extend and improve our thesis.

2 Background

This section aims to elaborate on the technologies used in developing the proposed provenance solution for handcrafted jewellery.

2.1 Blockchain

Blockchain is a data structure that consists of a chain of blocks which represent a transaction history or simply a digital ledger of transactions. Each block contains a cryptographic hash value of previous block, a timestamp, and a nonce - which is a random number for verifying the hash. This design ensures that any change on the block will immediately change the respective hash value. The initial block on the chain is referred to as a genesis block. For a block to be added on the chain, the network through a consensus mechanism has to agree on the validity of the transaction and the block. Swanson [2], describes consensus mechanism as “the process in which a majority (or in some cases all) of network validators come to agreement on the state of a ledger”. Therefore the consensus mechanism ensures that new transactions are stored in the block for a period before been added to the ledger. This means that the information cannot be altered later.

Blockchain can be classified as private or public. Private blockchains are made up of closed, predefined set of validators while Public blockchains allow anyone to join as a paid validator at any time. Even though private blockchains are preferred by business due to privacy and performance, public blockchains are trusted more since they make the assumption that unrelated people cannot collude and reach consensus on invalid data. Bitcoin and Ethereum are some examples of public blockchains. Bitcoin[1] is known for its decentralized cryptocurrency system while Ethereum[2] for its distributed computing platform featuring smart contracts.

[1] https://www.bitcoin.com/

[2] https://www.ethereum.org/

Use of cryptography in blockchain allows users to trust each other, thus there is no need of a central authority or intermediary to perform peer-to-peer transactions of different kinds of assets over the internet. Digital signatures are a form of cryptography and are used to ensure that transactions are only made by the rightful owners. Furthermore, blockchain's distributed nature ensures a fault-tolerant network, where the network persists even if a specific node breaks down, while, it's immutable nature, in which a block cannot be changed once added to the ledger, ensures auditability and integrity of the entire network.

2.2 Ethereum

Ethereum is an open generic blockchain platform developed by the Ethereum Foundation, a Swiss nonprofit organization[3]. It supports permissionless transactions on both public and private network, which means anybody is allowed to participate in the network. Ethereum works on the premise that all participants have to reach a consensus over the order of all transactions that have taken place and have access to all entries ever recorded.

A transaction is a valid state change that is identified by a cryptographic hash value or a transaction ID (TxID). A valid state change represents a move from an original state to final state. Invalid state changes which are often may include debiting an account balance without its corresponding credit. Final state can include information such as account balances, data representing information to the physical world etc. Transactions are grouped into blocks which are then chained together using a cryptographic hash as means of reference [3]. Transactions on Ethereum executed on the Ethereum Virtual Machine (EVM) which runs on blockchain.

To prevent double-spending transactions, Ethereum enforces a cryptographically secure proof of work (PoW) by miners. This is made possible by blocks possessing rewards that encourage miners to mine. Ethereum uses a currency known as Ether, also known as ETH, to transmit value to the miners as a means of incentivising computation. 1 ETH is made up of 10^{18} Wei, where Wei is the smallest unit of value for the Ethereum currency.

[3] http://www.ethdocs.org/en/latest/index.html

Every transaction in Ethereum network is digitally signed by the sender. The signing is made possible by a mathematical function that takes in a hashed value of some data object and a private key. To verify a signature, a reverse function takes a public key and the signature, then it compares it against the hashed value of the data object.

2.3 Smart contract

Smart contract is an instance of a computer program that runs on a blockchain. It consists of a program code, a storage file and an account balance. The program code is fixed when the contract is created and cannot be changed. A smart contract is invoked wherever it receives a message and executed by a network of miners who reach consensus on the outcome of the execution, and update the contract state on the blockchain accordingly. It can also receive money into its account balance and send money to other contracts or users. Contract state can only be trusted for correctness and availability but not for privacy since its publicly visible. Smart contracts are accessed via an Application Binary Interface (ABI).

Smart contracts use the concept of gas to control the consumption of resources. For a transaction to be created, currency in the form of ERC20 tokens must be used to purchase gas. If the gas runs out before the transaction reaches an ordinary stopping point, it is treated as an exception. At this point, the state is reverted as though the transaction had no effect, but the Ether used to purchase the gas is not refunded. When one contract sends a message to another, the sender can offer only a portion of its available gas to the recipient. If the recipient runs out of gas, control returns to the sender who can use its remaining gas to handle the exception and tidy up [4].

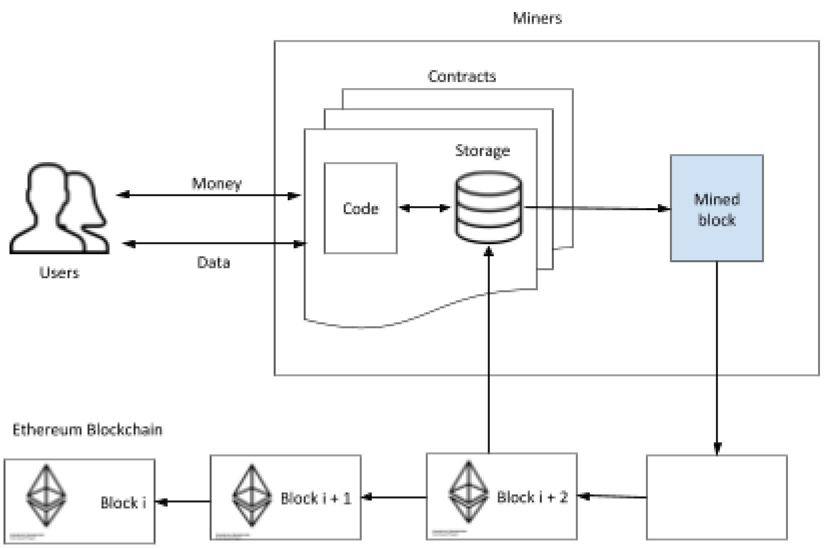


Figure 1. Smart contracts on Ethereum Blockchain

Smart contracts that require cryptographic signatures from multiple addresses so as to executed are referred to as multi signature (multisig) smart contracts. Ethereum smart contracts are mostly written using Solidity[4], a statically typed compiled language similar to javascript. Applications built on top of smart contracts are referred to as Decentralized Applications (dApps) and can be written in HTML, CSS or Javascript. These applications can be hosted on a decentralized file service such as IPFS[5] or a traditional web server.

2.4 Tagging technologies

Tagging is a mechanism mostly used in track and trace technologies to uniquely identify an item. The following technologies will be used to tag items across the supply chain.

2.4.1 Radio frequency identification (RFID)

This technology consists of three parts: a reader, antenna, and a tag. The reader has a microprocessor that is connected to an external computer. A radio frequency antenna is

[4] https://solidity.readthedocs.io/en/v0.4.23/
[5] https://ipfs.io/

connected to the reader and is used to transmit wireless radio signals to the tag or transponder. This antenna also receives radio signals reflected by a tag’s antenna in response [5].

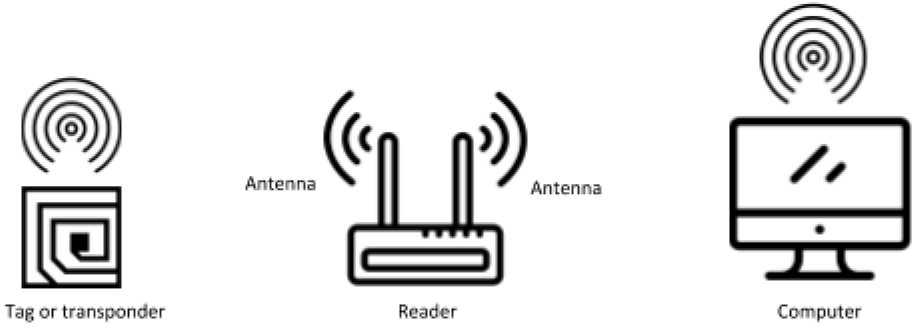


Figure 2. RFID setup

The tag has an inbuilt antenna which receives radio signals from a reader, a rectifier which converts the received signal to provide power to the tag, a memory in which the data in form of Electronic Product Codes (EPC) is stored, and an optional low power processor which is used to encrypt the data in the tag’s memory. EPC is a unique identifier that is used to distinguish products in the supply chain. Unlike barcodes, RFID tags do not need to be in the reader’s line of sight. This technology is commonly used in provenance solutions for tagging purpose.

2.4.2 Quick response (QR) code

A quick response (QR) code is two-dimensional code in square shape image, mostly represented by black and white pixels in a binary form. It’s mostly used in consumer advertising such as web pages and posters. QR code compared to barcodes have fast readability and better storage capacity. QR codes can be scanned by imaging devices such as smartphone cameras and processed using the Reed-Solomon error correction codes[6] until the image is fully interpreted. The result are matrices representing the image from which data is read.

[6] https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction

2.4.3 Near field communication (NFC)

Near field communication (NFC) is a short range wireless communication technology which requires bringing two NFC compatible devices within at least 4 cm range of each other. NFC technology enables two users to easily communicate and exchange data simply by touching two mobile phones to each other. This has enabled contactless payments, quick file sharing and electronic identity documents. Due to the touching paradigm, NFC ensures security of data since it's harder to tap or intercept the data within a short distance.

3 Related Work

In this section, we respond to our first research question - what is the state of art of blockchain-based provenance solutions? We start by presenting four approaches on how provenance has been implemented using blockchain technology in different domains. The following is our selection criteria:

1. Blockchain-based provenance solutions with literature materials detailing their implementation
2. A wide selection of blockchain-based provenance solutions with varied implementation
3. Blockchain-based provenance solutions implemented on a global supply chain

3.1 Provenance for diamonds

Diamonds are precious gems characterized for their lustre and hardness. They can also be classified by their weight, shape, clarity and color. Apart from their application in industries they also have a common usage in jewellery manufacturing. Currently, synthetic diamonds and those sourced from war zones (blood diamonds) are steadily proliferating the global diamond market. For a diamond stone to attain a conflict-free status, due diligence has to be applied to know its geographical origin; its source i.e. recycled, mined or synthetic; conditions of extraction; and labour practices involved [10]. This is referred to as provenance as it provides a proof of authenticity and a record of ownership. Provenance provides the basis of establishing traceability, which details the history of a piece of stone from the day it was mined to present day.

To support diamond provenance, key regulations and industry standards have been developed. Specifically is the Kimberley Process (KP)[7], which through its production and trade guidelines ensures rough diamonds from conflict areas do not fall into the hands of consumers. KP demands every diamond export to be accompanied by a certificate issued by Kimberley Process

[7] https://www.kimberleyprocess.com/en/what-kp

Certification Scheme (KPCS) [11]. Despite these measures, longer wait times for certifications (from 2-3 weeks to 3 months or more) and forgery of paper certificates are prevalent.

Everledger[8] has responded to this need by designing a Diamond Time-Lapse Protocol (DTLP)[9] solution that can be used to verify authenticity and custody of diamonds by use of blockchain technology. This solution creates a ledger to show the movement of diamonds with the following metadata: origin and source of mining; gems attributes such as carat and cut; processes such as cutting and polishing; artisan work; and certification. This metadata is then used to create a unique digital record on permissioned and permissionless ledgers. Permissioned ledgers limits accessibility and controls the access to private and confidential information to permissioned users only, while permissionless ledgers allow everybody to have viewing accessibility.

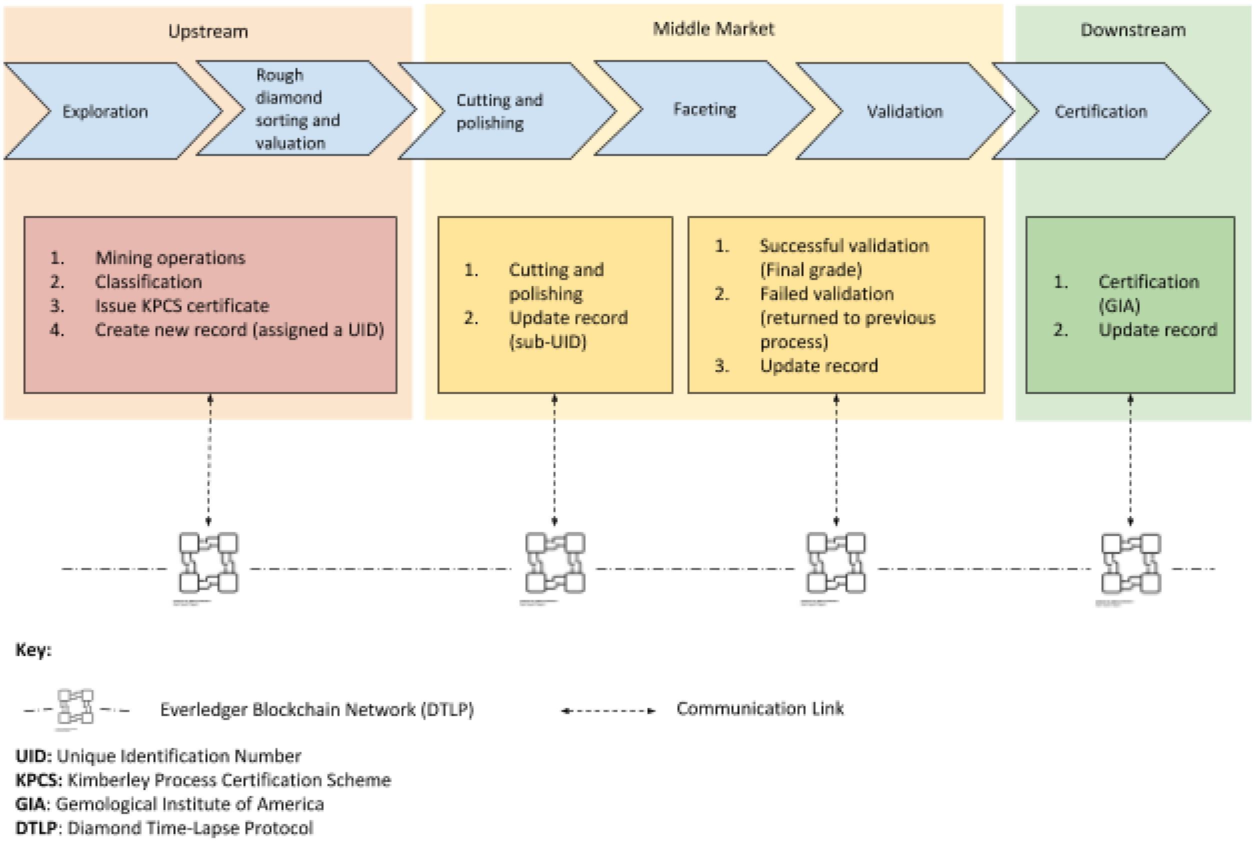

Upstream
Middle Market
Downstream
Exploration
Rough diamond sorting and valuation
Cutting and polishing
Faceting
Validation
Certification
1. Mining operations
2. Classification
3. Issue KPCS certificate
4. Create new record (assigned a UID)
1. Cutting and polishing
2. Update record (sub-UID)
1. Successful validation (Final grade)
2. Failed validation (returned to previous process)
3. Update record
1. Certification (GIA)
2. Update record
Key:
Everledger Blockchain Network (DTLP)
Communication Link
UID: Unique Identification Number
KPCS: Kimberley Process Certification Scheme
GIA: Gemological Institute of America
DTLP: Diamond Time-Lapse Protocol

Figure 6. Everledger DTLP provenance solution for the diamond supply chain

[8] https://www.everledger.io/

[9] https://diamonds.everledger.io/

The first phase in diamond manufacturing is exploration, this is where the rough diamonds are mined and classified by an expert based on their size, color, clarity etc. The KPCS issues a certificate for every mined diamond. With the Everledger solution, diamond metadata is captured and assigned a unique identification number before been stored in the blockchain. Diamonds are tagged so as to link them to their digital records.

The next phase is cutting and polishing. Cutting involves an experienced artisan guiding a machine on the best plan to cut the diamond by use of laser technology. Each of the new piece from the cut is assigned a sub unique identification number. Thereafter, the diamond pieces go through polishing or faceting. This is a complex process that requires experience and precision to scrub off unwanted surfaces from a cut diamond. The polished diamonds then go through the quality control process to be validated. Diamonds failing the validation process are returned to the previous process, while those that pass the validation process are given a final grade. Grading involves comparing a diamond piece to a set of master diamonds. Further, the diamonds are certified by the Gemological Institute of America (GIA)[10] laboratories through scientific analysis such as spectroscopy, morphology and crystal growth structure [12]. The certificate is eventually uploaded to Everledger blockchain network.

3.2 Tuna fish supply chain

According to the World Health Organization, fish protein is a vital nutritional diet as it accounts between 13.8% and 16.5% of the animal protein intake of the human population [7]. Supply of fish depends on a distribution network, which begins from a producer (fisher) and ends with a retailer or restaurant who then sells to a consumer. A distribution network normally consist of middle players who transform, package, and move a product from production to final sale.

Research by Future of Fish into the Indonesian Tuna fish supply chain, has revealed a lack of transparency and traceability that has encouraged unlawful practices, which contribute toward environmental degradation, abuse of human rights, and illegal fish supply.

[10] https://www.gia.edu/

The supply chain starts by remote fishers bringing in tuna fish to a common location, where middlemen can purchase and divide the stock for local and export markets. Local markets involve local processing and distribution networks, while export markets involve processing in Jakarta and distribution to Vietnam or straight to international markets [8]. The figure below shows the value chain of the Indonesian Tuna fish supply.

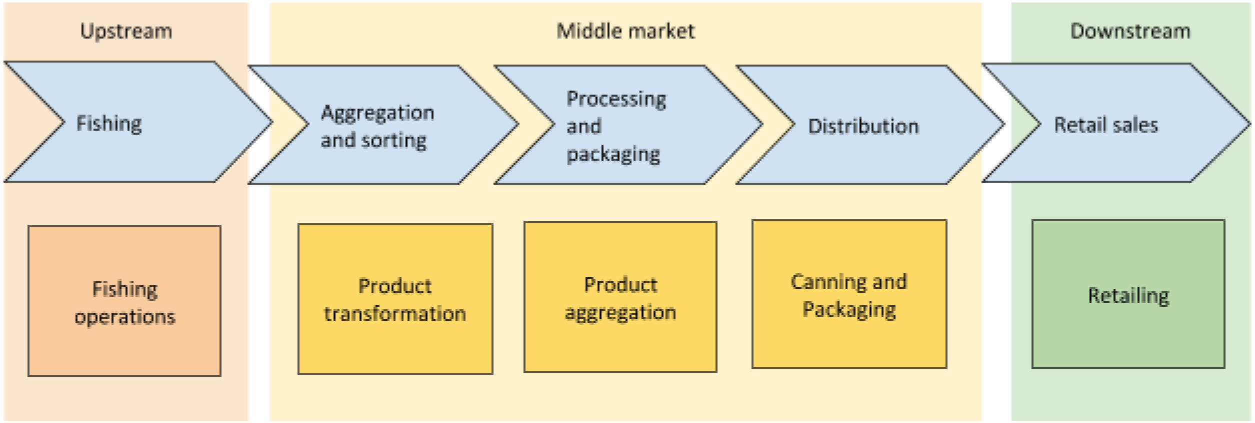


Figure 3. Indonesian Tuna fish supply value chain

The middle market processes can be expanded into the following major processes:

1. Paper receipt from the middleman to fisher
2. Middleman keep a written ledger of purchased products from fisher and sends the paper form to processor noting the transaction
3. Regulatory body perform paper-based dockside data collection into an Excel spreadsheet and upload to iFish[11] and government database
4. Local processor uses paper trail to follow the product

[11] http://www.ifish.id/

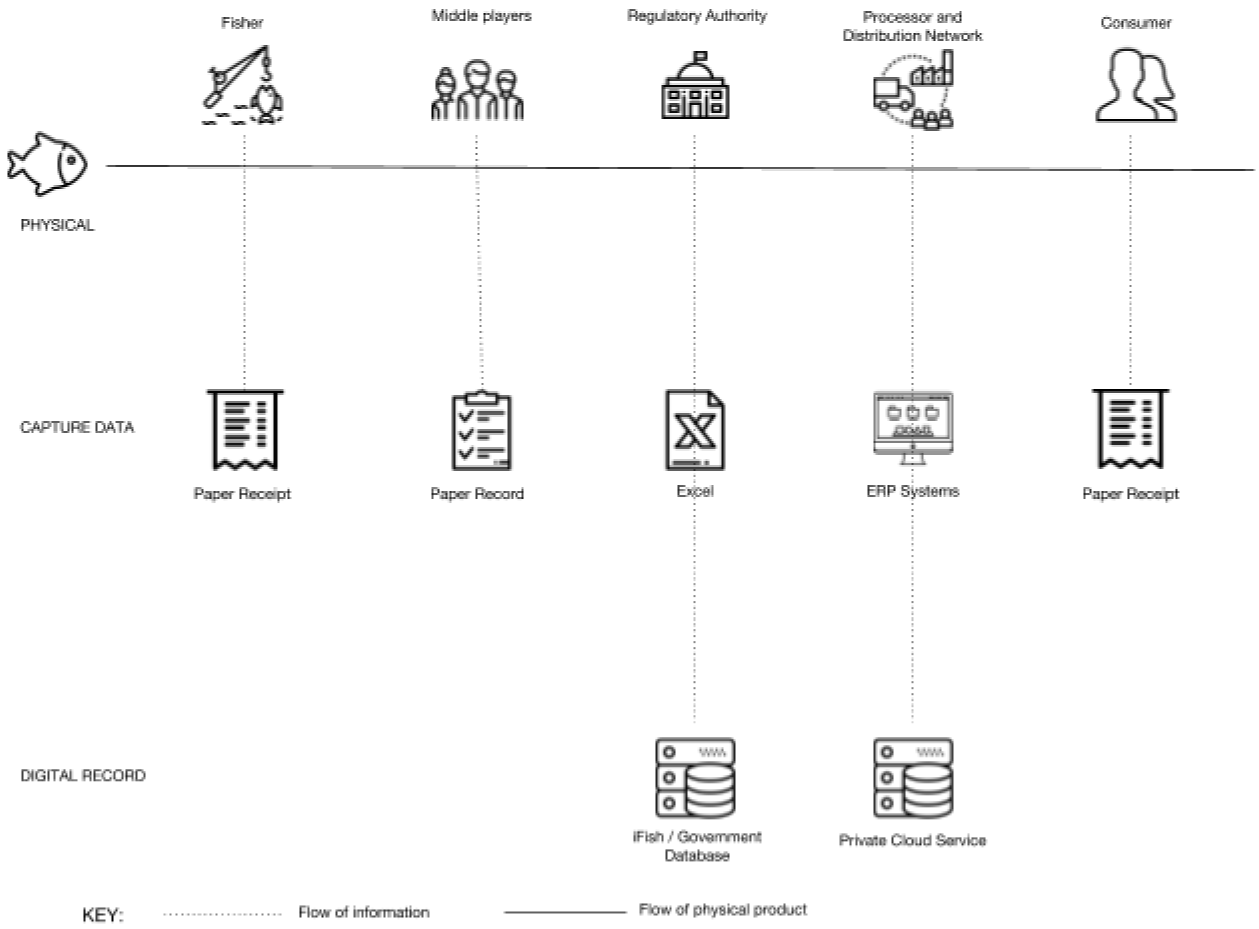


Figure 4. An illustration of the current Indonesian Tuna fish supply chain

However, the following provenance related issues arise from this supply chain:

1. There is a lack of record differentiating what was caught by each vessel in a fishing session.

2. Middle players trying to maintain a steady supply to their processors, end up aggregating fishes from multiple suppliers (fishers). They also transform the aggregated fish prior to data recording.

3. Possibility of data loss due to the use of manual records which are either hand-written or printed

4. Local processors aggregate products from different fishing events into a single volume. This makes it difficult, if not impossible to accurately determine origin of a catch, and extra provenance data such as catch method, or date of harvest.

5. Local processors and distributing networks use isolated systems which makes it hard to identify the flow of a product in the supply chain

To address the above challenges, Provenance.org[12] has presented a solution as a proof of concept to tracks Tuna fish from Indonesia to hotels in London. This solution focuses on enhancing traceability of aggregated fish products; resolving interoperability issues among different data silos and networks; establishing a consensus among users to agree on one single source of truth; and use of IoT and smart devices to capture data into the digital realm.

In the first mile of capturing data, fishers (producers) are to send a short message service to register their catch. Each message is recorded as a new asset entry on the underlying blockchain network. The data on blockchain is then transferred from fisher to supplier, both physically and on the blockchain network. The identities of the fishers are immutably stored on a chain of transactions in the network.

During processing, the fish are aggregated from different suppliers and transformed into new products. Transformation includes cutting the fishes into pieces and packaging pieces from different fish into the same can. Since the each fish as a whole was initially registered on the blockchain network, the transformed fish is once again updated on the blockchain by use of smart contracts. This is achieved by sending the mass balance values from Tally-O[13] system to the smart contract once transformation has taken place [9].

Since, majority of the processors and distributors already have a enterprise resource planning (ERP) and data management systems. To interconnect these heterogeneous systems, Blockchain provides us with a single source of truth (SSOT) which supports sharing of data across different systems, allowing distributed mass balancing of fish to be conducted. In addition, data is

[12] https://www.provenance.org/
[13] http://thisfish.info/

securely stored and transmitted thus ensuring authenticity without the need of changing existing data capture interfaces.

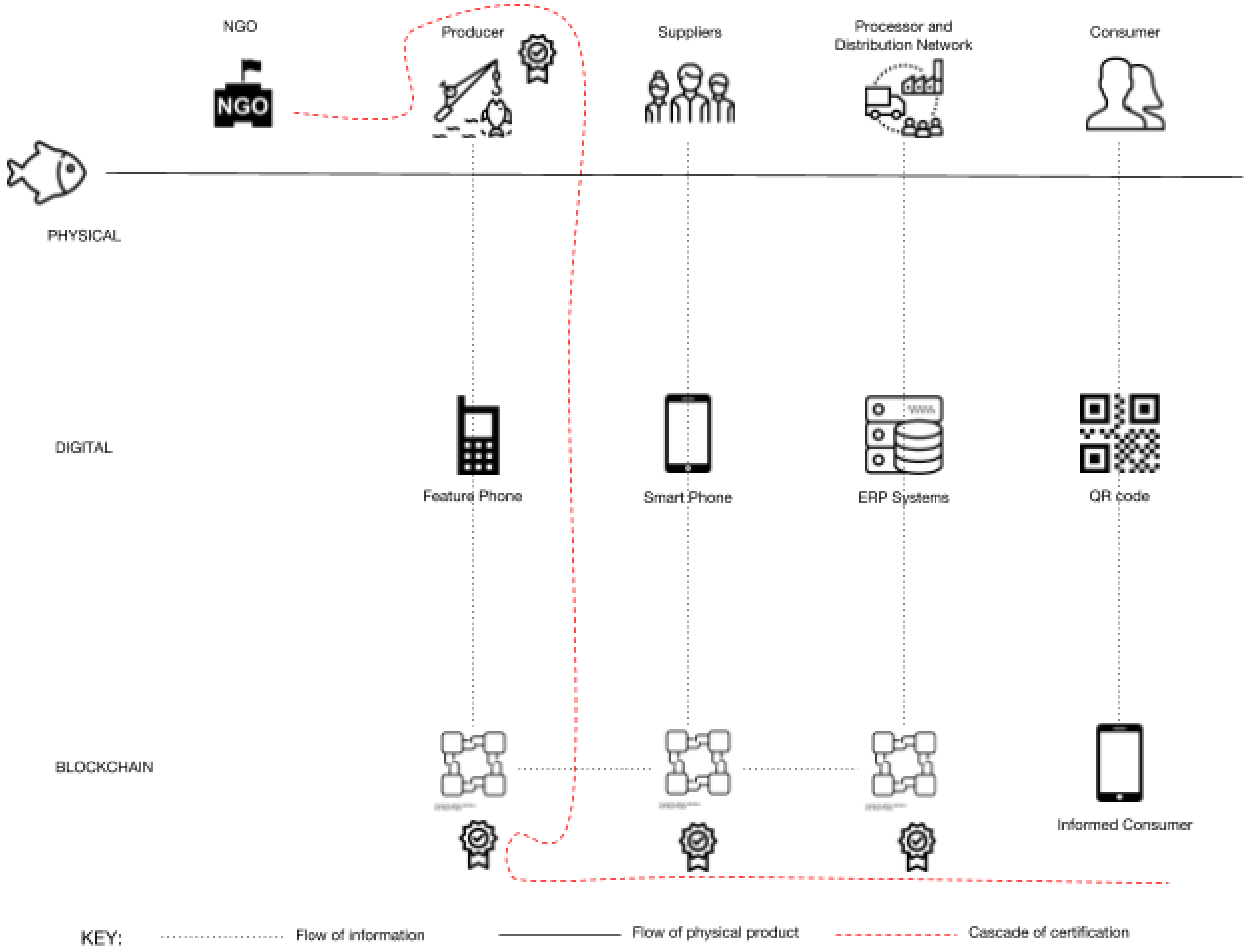


Figure 5. Indonesian Tuna fish supply chain Blockchain-enabled provenance solution

Across the supply chain, to link fish products to their digital records, QR codes and NFC smart stickers are used for tagging. Consumers can then use a mobile app to scan NFC-enabled smart stickers or browse in-store tablets to retrieve provenance information about a product.

3.3 Anti-counterfeit solution for medical products

The World Health Organization (WHO) describes counterfeit as a false representation of an actual medical product in relation to its identity or origin. Identity misrepresentation refers to misleading statements with respect to name, composition, strength etc. whereas origin misrepresentation refers to any false statements with respect to a manufacturer, country of origin, or an authorisation holder. Counterfeit medical products result not only to loss of revenue or intellectual property but also pose a serious threat to public health. WHO estimates 1 in 10 medical products in low and middle income countries is substandard or falsified [13]. This has lead to more than 1 million deaths reported every year as per the International Criminal Police (Interpol) [14]. This presents a need of having a way to authenticate and proof the origins of a medical product.

Modum[14] has designed a blockchain enabled track and trace technology solution that monitors temperature conditions of medical products while in transit. Track and trace technologies allow systems to assign a unique identity to each stock unit during manufacture which then remains with it through the supply chain until its consumption. This unique identity is securely stored in an accessible database with its related metadata [15]. Track and trace technologies include serialisation, barcodes and RFID tags.

This solution is an early proof of concept that seeks not only to enable companies in the pharmaceutical industry to comply with the European Commission guideline on Good Distribution Practice (GDP) of medical products for human use [16], but also provide provenance information that consumers can rely on.

The modum system is made up of a frontend and backend system. The frontend system comprises of dashboards, pharmacy qualified temperature loggers, and a mobile application. The backend system runs an Ethereum node for executing smart contracts. It also has HTTPS server to serve data requests and a database for storage. The frontend system communicates with the backend via JSON Rest API. The figure below illustrates the implementation

[14] https://modum.io/system/

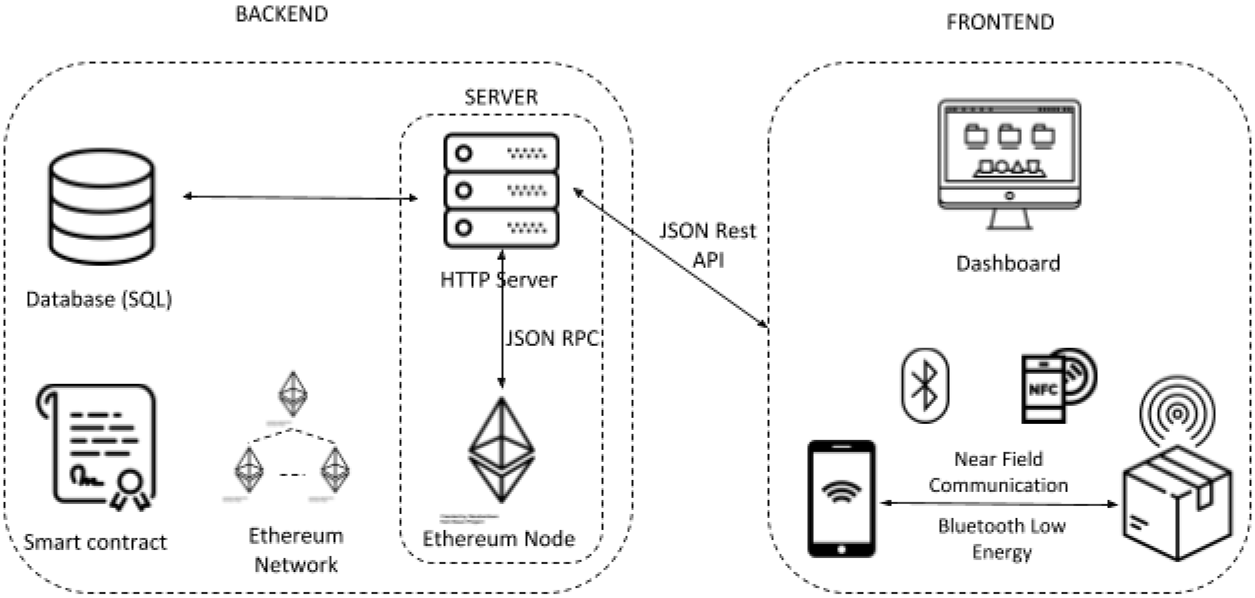


Figure 7. Modum system architecture

The temperature logger monitors the temperature condition of medical products while in transit. It also transmits the data to a mobile application via BLE (Bluetooth Low Energy) or NFC (Near Field Communication). The dashboard provides a visual representation for the user to view shipment tracking information. It also supports setting of an alarm criteria, data visualization and analytics. The mobile application can be used to read information from the temperature loggers, initialize shipment transactions and visualize the data.

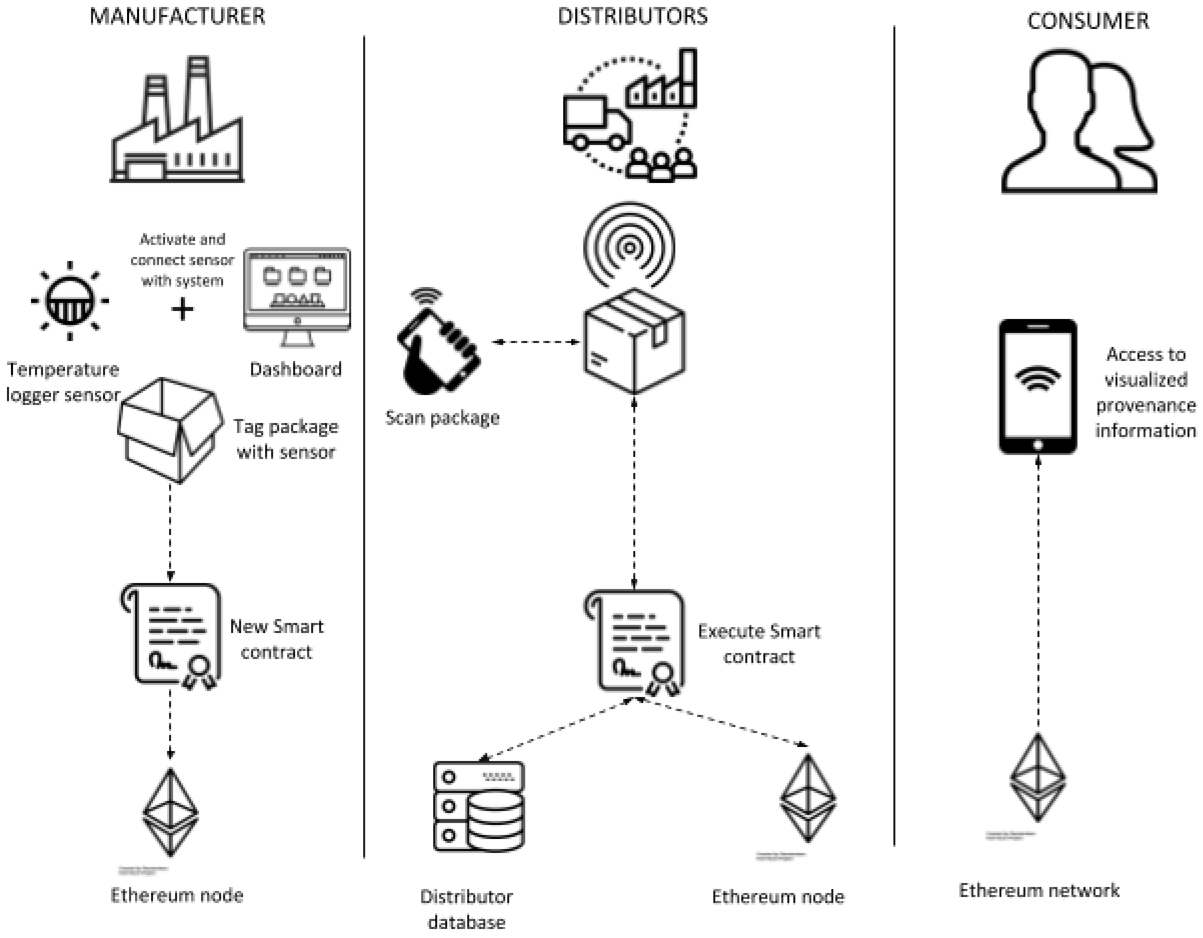


Figure 8. Illustration of a blockchain enabled track and trace technology

Before the shipment process begins, data such as shipment tracking information, temperature logger serial number, measurement intervals, and temperature ranges (alarm criteria) are recorded in a shipment specific smart contract. The alarm criteria is used to evaluate if in transit temperature conditions are as per the GDP regulations. The loggers can then be queried for the current shipment temperature data by the use of BLE or NFC technology without the need of opening a package. The data is submitted to the backend system to be validated for authenticity and compliance by a shipment-specific smart contract without the possibility of any party to interfere. The results of the evaluation including a pointer to the actual measurement data stored in a SQL database, and a hashed yes/no outcome with respect to the preset temperature range, are mapped to a public blockchain network as a proof-of-existence. Users are also notified of any deviation and can review the corresponding measurement and shipment data.

3.4 Authentic Art and Collectibles

Artists attach too much importance in identifying with their works, similarly, collectors are concerned with possessing a good title for their collectibles. However with the current solutions, verifying the authenticity of a piece of art or establishing a good title is an ad hoc and unreliable practice. This rises from the fact that there is no central registry similar to the one used in the house rentals market. Moreover, collectors are unwilling to trust a central entity with their ownership data while intermediaries such as auction houses are not willing to risk losing their position.

Provenance facilitates proper and reliable documentation for the current ownership of a piece of art or collectible which helps to facilitate transactions such as buying or selling, while a record of past ownership stands to prove its authenticity and value. Traceability on the other hand describes the history of an item from the day it was created to present. Collectors rely on provenance to know whether an item they are buying is authentic, whether the seller has the right to sell it, or to identify the rightful owner for insurance purpose.

The ideal provenance for a piece of artwork or collectible refers to a well documented history of ownership in an unbroken chain of transmission since creation. In the case of antiquity objects, provenance refers to its documentation since it was found, unearthed, or at least since sold by a trusted intermediary. In summary, good provenance for arts and collectibles should support:

1. Secure and reliable transfer of ownership or a legal title
2. Asset-backed lending since lenders can confirm valuation, authenticity and title
3. Improved insurance products
4. Royalty payments for creators

5. Guarantee authenticity for future works

Blockchain technology can be used to enhance provenance by providing a decentralised, anonymous and trustless network where data is recorded in an immutable nature. It can also provide an opportunity to trade art with digital currencies, and support fractional ownership.

Codex[15] has implemented a title registry on the blockchain network, known as The Codex Protocol Title Registry. This consists of a Codex Title, which is a token that represents ownership and transactional history of an item since it was instantiated. It also includes hashes of related documentation such as sales receipts and written appraisals from experts. The benefit of having a title is that it can be used to verify current ownership and determine an items value. Furthermore, the codex title can be used in title-deposit escrow smart contracts to facilitate easier transfer of ownership. The Codex title registry can be used to implement an arts and collectibles trading market, as shown below:

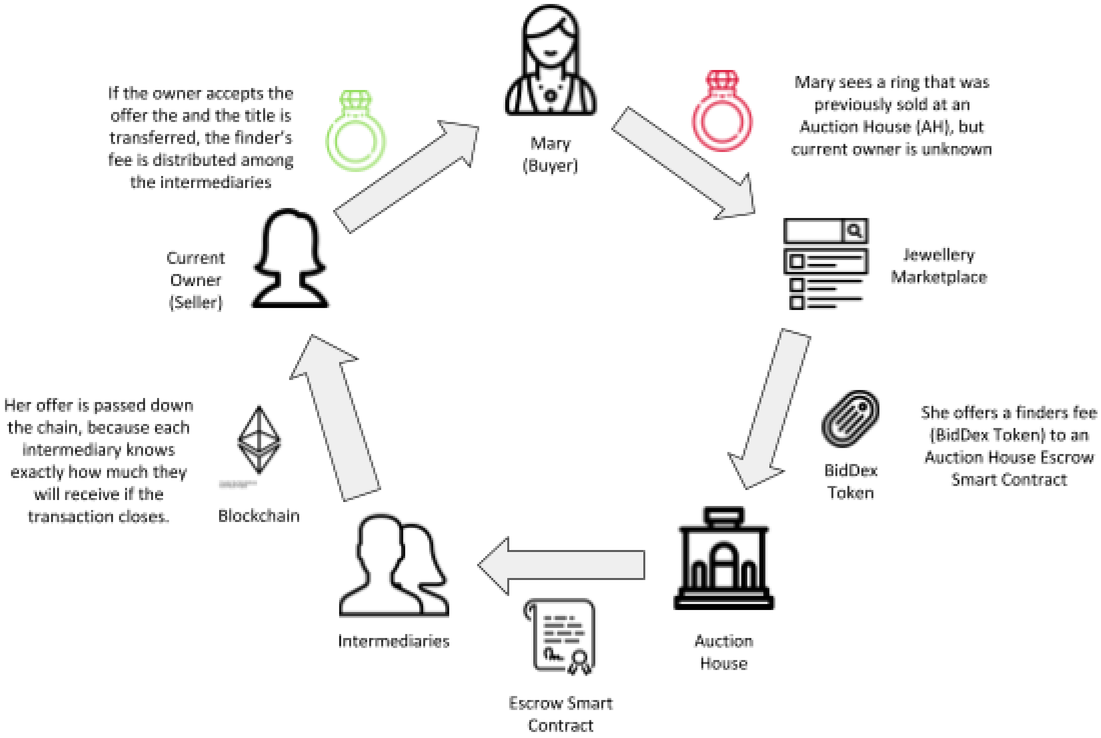

Mary (Buyer)
Mary sees a ring that was previously sold at an Auction House (AH), but current owner is unknown
Jewellery Marketplace
She offers a finders fee (BidDex Token) to an Auction House Escrow Smart Contract
BidDex Token
Auction House
Escrow Smart Contract
Intermediaries
Her offer is passed down the chain, because each intermediary knows exactly how much they will receive if the transaction closes.
Blockchain
Current Owner (Seller)
If the owner accepts the offer the and the title is transferred, the finder's fee is distributed among the intermediaries

Figure 9. Sellable dApp implemented on top of Codex Title Registry

[15] https://www.codexprotocol.com/

In this registry, a buyer cannot see the identity of owners who elect to remain private. However, they can ask existing public entities in the registry such as auction houses to communicate their purchase offer at a cost, which is traded in their own token known as BidDex. The Codex Title is modeled as an ERC-721 Non-Fungible-Tokens (NFTs)[16], which implies that any changes to the title will be recorded on the blockchain. NFTs are inherently different from crypto-currencies where each token is interchangeable and tracked on the blockchain as a count rather than as an individual token. Both Codex Title and BidDex tokens are built on the Ethereum blockchain [17]. However, the challenges with this Codex implementation are:

1. Items already are in existence will have immutable history from the point they are instantiated on the Codex registry. This means there will exists black holes of relevant information that can only be relied from the Auction houses
2. Fidelity in mapping of physical items to digital records. Probable solution to this challenge is that in case of forgery, buyers have the option to reverse search for an existing title

3.5 Discussion

We conclude this section by discussing the above solutions and provide an answer to our second research question - what are the key features for designing a blockchain-based provenance solution?

1. Metadata

Metadata represents the descriptive and structural properties of an object and can be used to show the existence of provenance. For metadata to be captured, there has to be a way to identify and describe an object. Attribute identification is one mechanism that allows us to describe both the intrinsic and extrinsic properties of an object so as to allow us create its digital record. For instance, the Tuna fish case study uses attributes such as the species name of a fish, location, mass, and fisher identity to capture provenance data at the first mile of the supply chain.

[16] https://github.com/ethereum/eips/issues/721

Similarly, the diamond case study describes how attributes such as size, clarity, color, carat and cut have been combined with other attributes such as source location to create a digital record of diamond provenance on Everledger's blockchain network.

2. Tagging

Once data has been captured, there has to be a mechanism to physically link products and the data. Tagging provides this mechanism by allowing a label attached to an item to act as a reference. An effective tagging solution should be nearly impossible to copy; be tamper evident; verify quickly via readers; should allow product description to be checked; and provide legal enforceable evidence. The provenance solution described in the Tuna fish case study uses QR code and RFID smart tags to physically link a fish to its digital record on the chain. In the diamond solution by Everledger, unique identifiers are used to tag a piece of diamond. Cut diamonds are further tagged by sub-unique identifiers which are linked to a blockchain asset. Likewise Modum's solution uses serialisation, barcodes and RFID tags to link medical products to their track and trace blockchain enabled solution.

3. Transparency

Transparency can be defined as the visibility on products metadata by other members of the supply chain and by consumers. Products metadata include their source of origin, processes they went through, parties responsible, certifications or licenses. It allows the users to determine whether practices or processes a product underwent complied with particular requirements. In the diamond case study, transparency is supported by Everledger's diamond time lapse solution, where on submitting a query of a unique identifier to a diamond piece, the system displays a provenance story[17] from the time the stone was mined to the point it was certified ready for retail stores.

4. Data verification

Verification of data is the ability to validate and confirm product information along the supply chain with data provided by trusted third party sources. If the verification process involves an

[17] https://diamonds.everledger.io/search/QSLIS013#close

identity or access to a resource, then it is referred to as authentication. Digital signatures and access controls provide a mechanism to verify and authenticate. In the authentic art and collectibles solution, provenance information about a piece of art can be verified by validating digital signatures.

5. Single source of truth (SSOT)

The aim of provenance solutions is to ensure data remains intact from origin to consumer. Single source of truth presents a data modelling architecture where data is stored exactly once. This means that all other data points act as a reference to a single primary source of truth. Thus, having a common backend with shared language and public infrastructure supports traceability. Public blockchain network provides this common backend through its immutable nature, consensus mechanism, and accessibility. Thus, it should be the ideal candidate for a SSOT to verify and validate provenance claims. This is supported by the above solutions all using blockchain technology to guarantee provenance.

4 Contribution

In this section, we respond to the third research question - how can blockchain technology guarantee provenance for handcrafted jewellery? We also present a case study of Soko, Inc. - a global handcrafted jewellery supply chain company. We describe their As-Is business process model and design a To-Be business process model that guarantees provenance using blockchain technology.

4.1 Handcrafted jewellery

Handcrafted jewellery refers to jewellery assembled by use of tools that are controlled by hand rather than use of manufacturing machinery. Handcrafting is a composite and complex process that requires highly skilled labour. That is, a lot of time and skill in designing and handcrafting unique pieces. Artisans generally go through years of apprenticeship to learn and perfect on their skills. The standard of a craftsman's ability is shown by the artfulness and style of the designs in their jewellery, and this carries the unique story and personality of an artisan. As a result of their reputation being at stake, artisans mostly aim at producing high quality jewellery by use of sustainable and ethically sourced materials.

Production of handcrafted jewellery happens mostly in small scale resulting in unique and very limited editions of the same product. In fact, most of the worlds finest and personalized jewellery is handmade. When consumers buy handmade jewellery they end up not only acquiring unique products but also connecting with the artisans and supporting their trade.

Provenance helps us identify who is the creator of a piece of jewellery, its origins and source of raw materials, processes it underwent and who claims its ownership or good title. Therefore, it can have a significant influence on the authenticity and value of a jewellery, mostly when its associated to a famous owner or renowned designer or craftsman, including its current ownership.

4.2 Case study

Soko, Inc[18] is a global women accessories global supply chain company with its production office in Nairobi, Kenya and sales office in San Francisco, USA. The company has specialised in bulk production to fulfill their fast fashion demand. Their business model is built around distributed manufacturing, which relies on business processes that put sparse entities together to achieve a net customer-driven goal. That is, they focus on fulfilling product and demand responsiveness through managing their distributed materials and production resources.

Soko has connected over 200 independent workshops around Nairobi and its environs. Workshops are owned by artisans and are operated as a sole proprietorship, partnership or limited company. The size of a workshop is averagely 1 - 5 persons. Soko's business operations are aligned towards ethically producing beautiful handcrafted jewellery. They manage this by ensuring that the materials artisans use are locally and eco-friendly sourced. Materials may include reclaimed cow horns and bones, recycled brass etc. In addition, they have developed training programs that guide the artisans to standardize on their quality and capacity.

Soko has also developed a cloud based software system that centrally manages sales orders (SO) and issues purchase orders (PO) to artisans. In addition, they have developed a mobile app that allows artisans to accept purchase orders, manage their inventories, and get paid through a mobile payment platform – m-pesa[19]. The orders contain design specifications which the artisan infuses with their own minimal aesthetics as a brand signature. Once a purchase order is due, artisans deliver their quantities in small batches which are then validated by a quality and assurance (QA) staff from Soko. Deliveries are normally done through Field officers (FO), however, artisans can opt to deliver by themselves. Once validated, the products go through a Work in Progress (WIP) phase, where they improve their value through electroplating, modification or assembly process. Thereafter, the products are batched up as per sales order

[18] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=261339091

[19] https://www.safaricom.co.ke/personal/m-pesa

requests and shipped to their distribution centers or directly to customers. Figure 10. below shows Soko's handcrafted jewellery value chain.

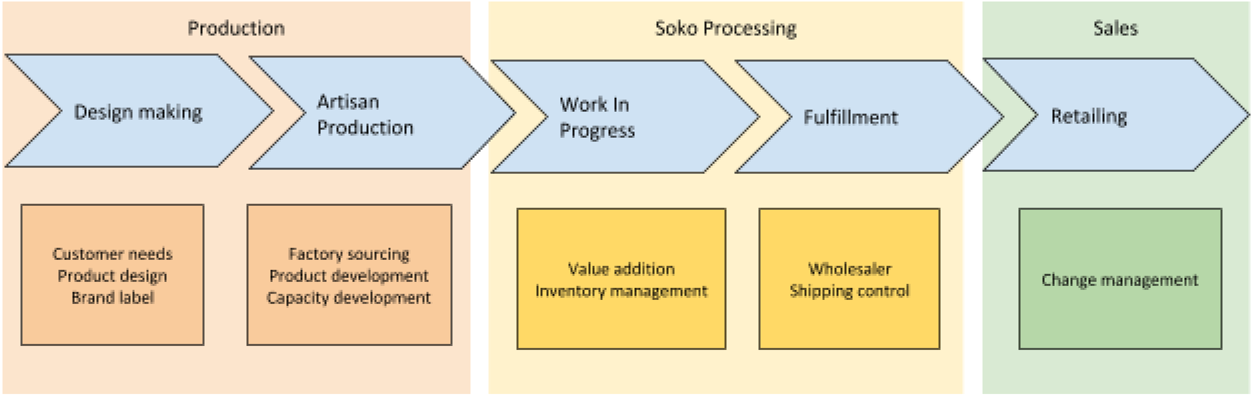


Figure 10. Soko's handcrafted jewellery value chain

4.3 As-Is Process Flow

Soko's handcrafting jewellery process starts with the design making process. This is where a designer collaborates with a skilled artisan to transform a concept into a real handcrafted jewellery. The design concepts are ideas sketched on paper or by a computer-aided design (CAD) software, including their dimensions and specifications. Design making process is a creative and iterative process. New designs normally go through a prototyping process, where the original design is transformed into a prototype to be tested by consumers. However, already approved designs skip the prototyping process and go to the next phase of production. See figure 11 and 12.

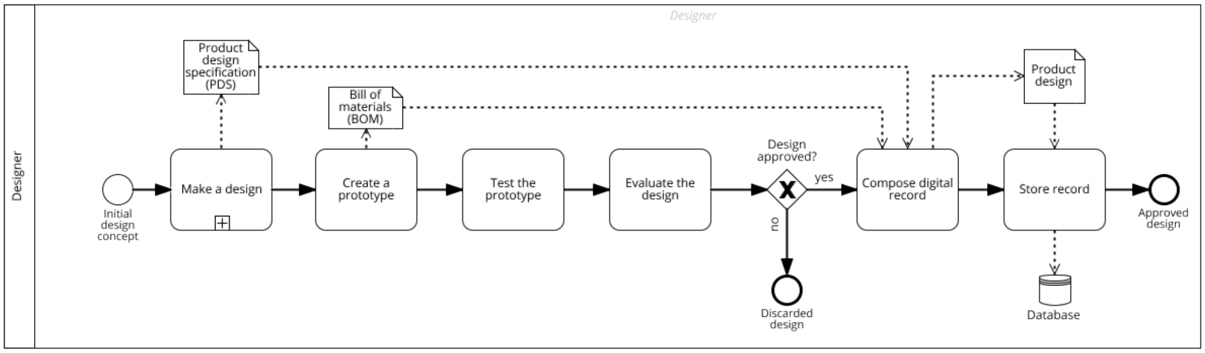


Figure 11. As-Is design making process

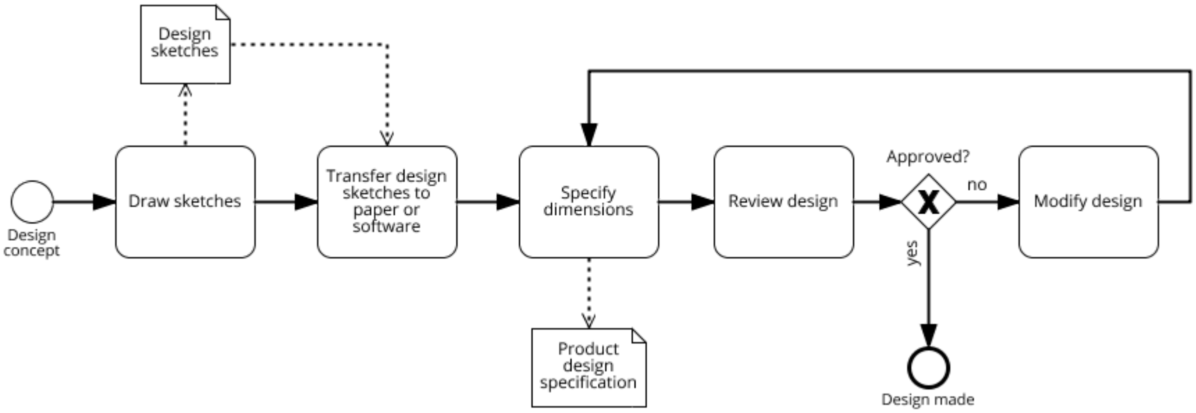


Figure 12. Make a design sub-process

The production phase involves a number of processes that rely on techniques such as casting, shaping, distortion, crimping, carving, punching, gluing, studding, flattening etc. Depending on an items specification, they can go through a custom sequence of processes. For instance to produce a cast piece item, the main process is casting. This is where liquefied metal is poured into cavities of a mold with the shape or form of articles to be produced. Lost wax is the commonly used casting technique where wax is turned into a mold and lost during the actual casting process. The result is a cast piece with excess metal on the surface. Filing technique is used to even out the surface or to shape the form. Most items from the custom process go through the polishing process so as to achieve the highest degree of smoothness. But specific items made out of horn or leather go through grinding and buffing processes respectively.

Once production is done, the artisan delivers the items to the nearest collection center, where field officers from the organization forward them to the headquarters. Received items are first validated by a quality and assurance (QA) staff member against some quality control measures. Items approved are taken into the work in progress (WIP) phase, which involves electroplating, modification or assembly process.

Electroplating is the coating of a metal with another metal such as copper or chromium through an electrodeposition process. However, items which require readjustment or tweaking go through the modification process. In case of an assembled product, the components go through the assembly process where they are fitted together to form the final product. Thereafter, finishing is applied for a soft and smooth touch. Quality checking is performed again and the approved items are forwarded to the inventory for storage. All rejected items are returned to the previous issuing process to be reworked on or discarded. Finally, all items from different purchase orders are aggregated per product type to be stored in the inventory.

In the event of a sales order is been almost due, items are pulled from the inventory to satisfy the sales order. Personnel from the fulfillment department receives the items and carefully packages them into respective boxes in order to avoid any sort of damages. A final validation and auditing process is done to ensure packaged items meet customers specifications. If they do, they are packaged, labelled and shipped to distribution centers or directly to customers. Figure 13 shows the As-Is business process flow described above.

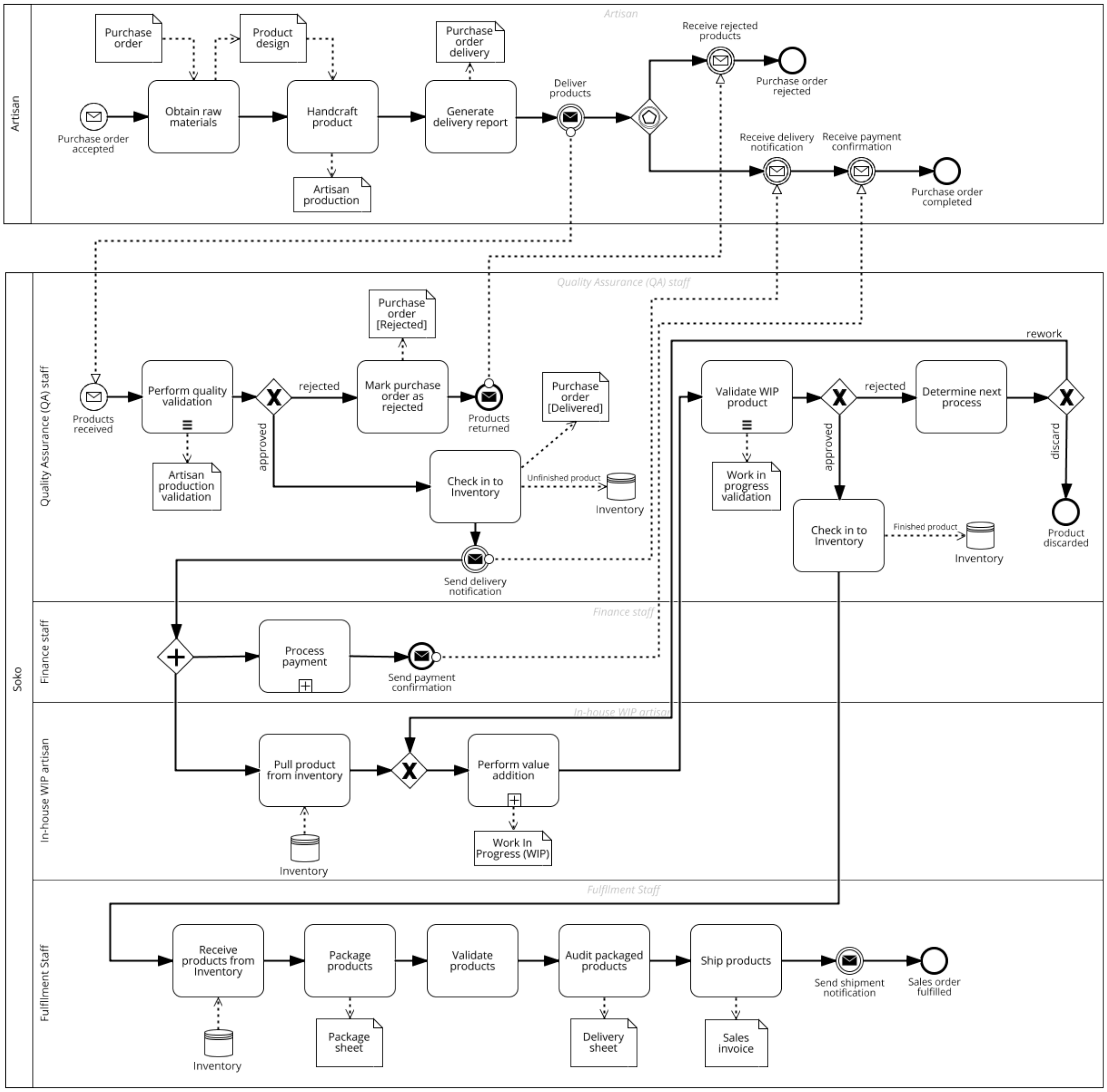


Figure 13. Soko’s As-Is handcrafted jewellery process flow

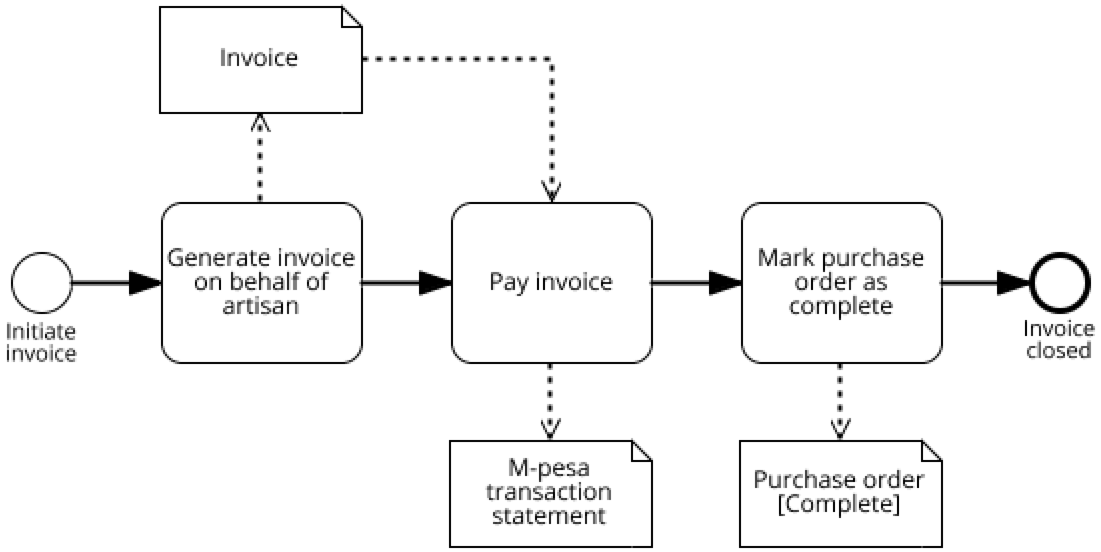

Invoice
Initiate invoice
Generate invoice on behalf of artisan
Pay invoice
Mark purchase order as complete
Invoice closed
M-pesa transaction statement
Purchase order [Complete]

Figure 14. Process payment sub-process

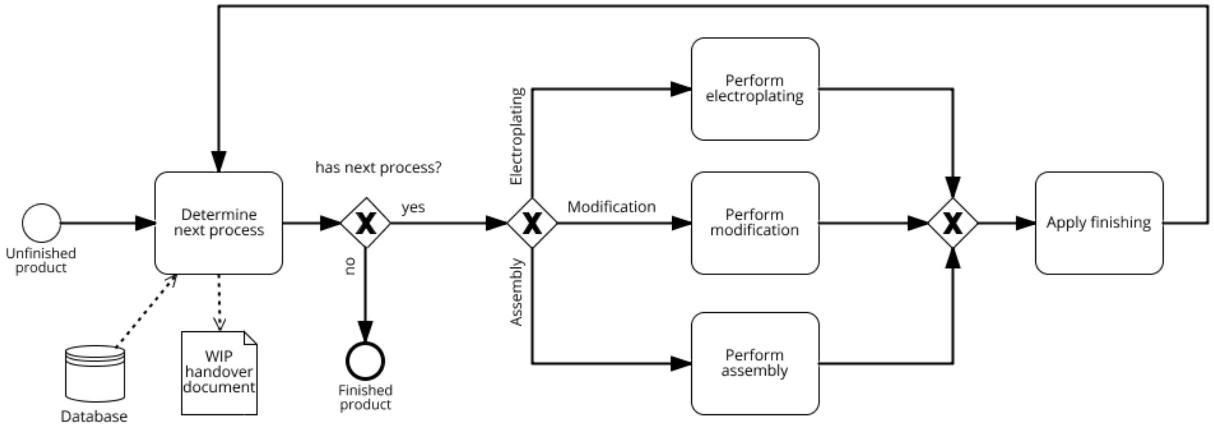


Figure 15. Perform value addition sub-process

4.3.1 Issues

The handcrafted jewellery global supply chain demands transparency and traceability so as to validate quality and assess ethical compliance. Transparency refers to visibility into the materials and labor practices used across the supply chain while traceability allows a product to be traced across the supply chain. Provenance forms the basis of guaranteeing transparency and traceability.

However, the current Soko implementation fails to guarantee provenance for its handcrafted jewellery. For instance, consumers have to rely only on the labels attached to the jewellery, which don’t have much information about the history of the product such as the source of raw materials, the processes it underwent or labour practices. Thus, they cannot verify if what they are paying for is genuine or as to whether they are supporting a legitimate course. On the other hand, artisans don’t have the visibility of who owns their jewellery let alone where it is on the planet. The reasons to lack of provenance can be summarised as:

1. Lack of documentation to the sources of raw materials and their origins.
2. Designers who create the product design specifications are not credited.
3. There is no way of identifying a piece of jewellery with a specific artisan due to aggregation at the inventory check in process.
4. The processes a product undergoes through are not captured and presented in a way visible to the consumers.
5. Tagging is not applied at all stages in the value chain thus hindering traceability.
6. The available provenance data is centrally managed in the company’s database. This raises questions of trustworthiness of data due to the possibility of data manipulation.

4.4 To-Be Process Flow

To address the above issues, a To-Be process flow will be designed. The objective would be to create a provenance solution for handcrafted jewellery using blockchain technology. The following assumptions have to be first considered:

a. Provenance scope will cover from ideation to delivering an item to a store. This allows this research to focus on the first phase of enabling provenance.

b. Generation of a purchase order (PO) and sales order (SO) will be out-of-scope. This is because purchase and sales order don't output data for provenance rather they are used as data inputs.

c. Ensuring the security of our tagging mechanism will be out-of-scope, since this thesis does not cover the hardware implementation.

d. Since all transactions executed by smart contracts require Ethereum tokens (ETH) to store data on blockchain or make payments, trading of digital currency (tokens) to fiat currency will be out-of-scope.

The following presents the To-Be process flow as per major activities:

1. Design making process

The design making process generates a product design specification (PDS) and bill of materials (BOM) records. The PDS record details all the dimensions and specifications of a product while the BOM record lists all the materials and techniques used in making a product. Both records are used to create a Product design record which includes the designers profile and is digitally signed. The resulting cryptographically hashed data is then committed to a smart contract which stores the record on blockchain (see figure 16).

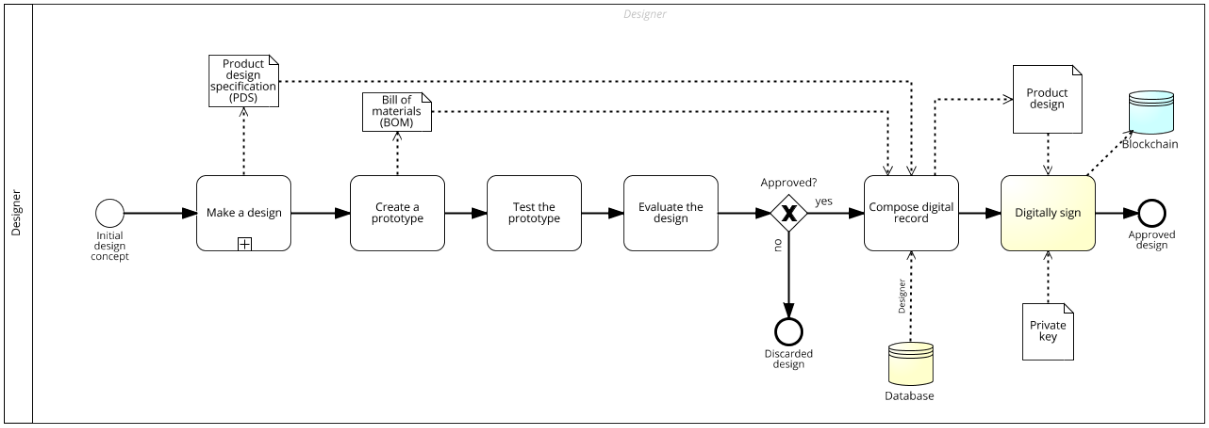


Figure 16. To-Be design making process

2. Production process

The production process generates an artisan production record that includes the quantity of items produced and a list of raw materials including their sources. It also details the production location, date and time updated. The product here is linked to a product design already existing on the blockchain through a Purchase Order Product record. Once the items are ready to be delivered, a Purchase Order Delivery record is generated showing the amount and serialized list of items delivered. This record acts as a handover document between the artisan and the organization (Soko). Both records are digitally signed by the artisan and committed to a smart contract on the blockchain network for storage.

3. Validation process

This process involves the quality and assurance (QA) staff validating the products delivered and either approving or rejecting them. Items received from external artisans once validated generate an Artisan Production Validation record. Whereas items received from work in progress process generate a Work In Progress Validation record. Items refers to serialized inventory items related to a purchase order delivery or a work in progress record. Rejected items are generally analysed to determine if they will go for a rework or they will be discarded. The QA staff performing the validation has to digitally sign the validation record and commit it to a smart contract that stores the record on blockchain.

4. Work in progress

The work in progress (WIP) is a phase where value addition is applied on products. Value addition can be achieved through electroplating, modification or assembly processes. WIP is essential to guaranteeing provenance as it provides all processes applied to the transformation of a product. The WIP record is digitally signed by an in-house WIP artisan. A new transaction is generated and committed to a smart contract for blockchain storage.

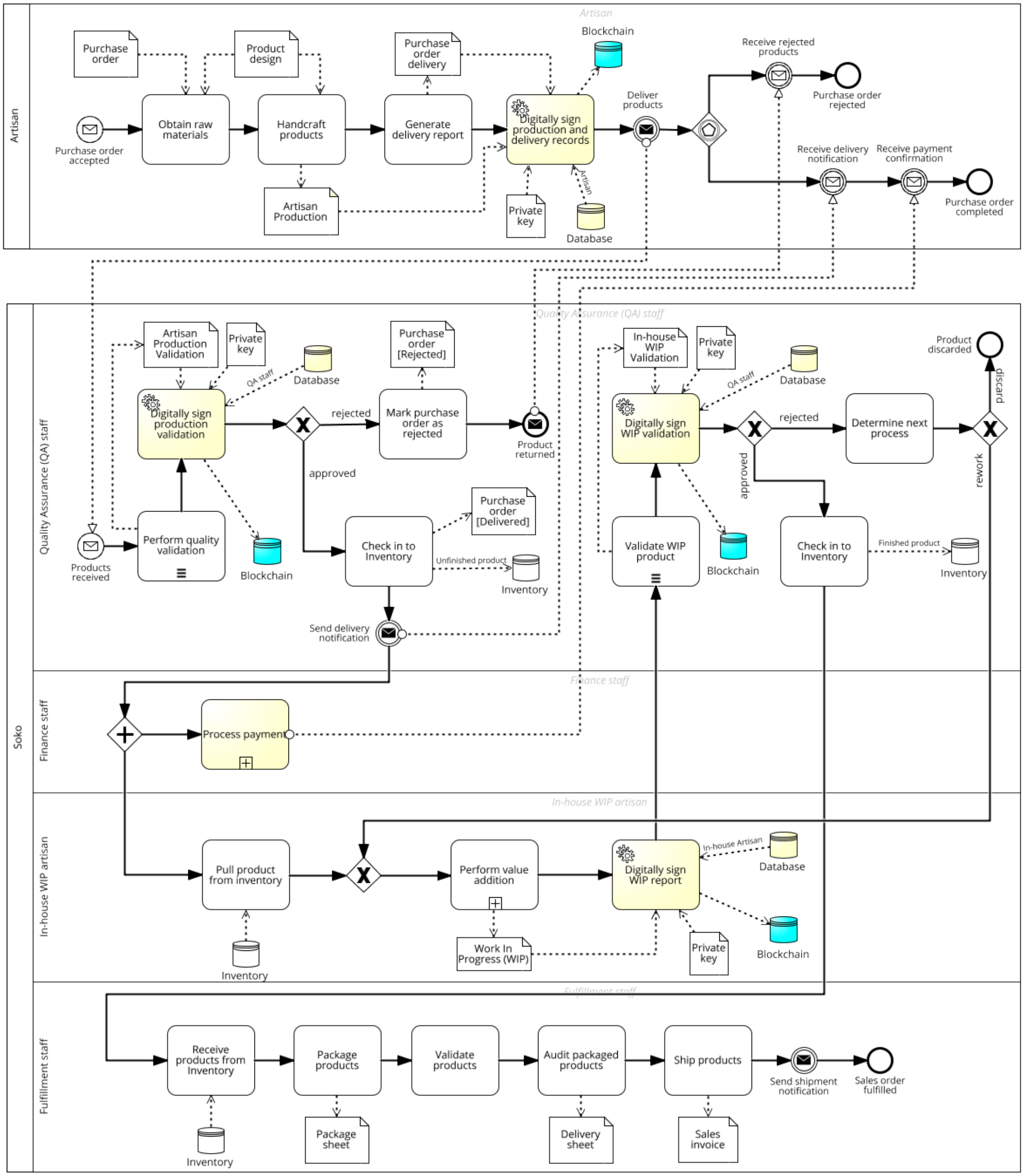


Figure 17. To-be handcrafted jewellery process flow

5. Payment process

Once products are approved and checked into inventory, the payment and value addition processes are initiated. The payment process awaits for an invoice from the artisan, which once received, the amount and particulars are confirmed against the purchase order. If approved, the invoice payment process is invoked. This process creates a multisig smart contract and a staff from finance department has to deposit funds as per the delivery payout in the purchase order and digitally sign the contract. Thereafter, the artisan receives a notification with transaction ID, which he has to confirm the payment by digitally signing the smart contract. The smart contract determines whether the condition is met and transfers the funds to the artisans account. It also transfers the title of ownership to the sender of the funds (buyer). These transactions are committed to a blockchain ledger (see figure 18 and 19).

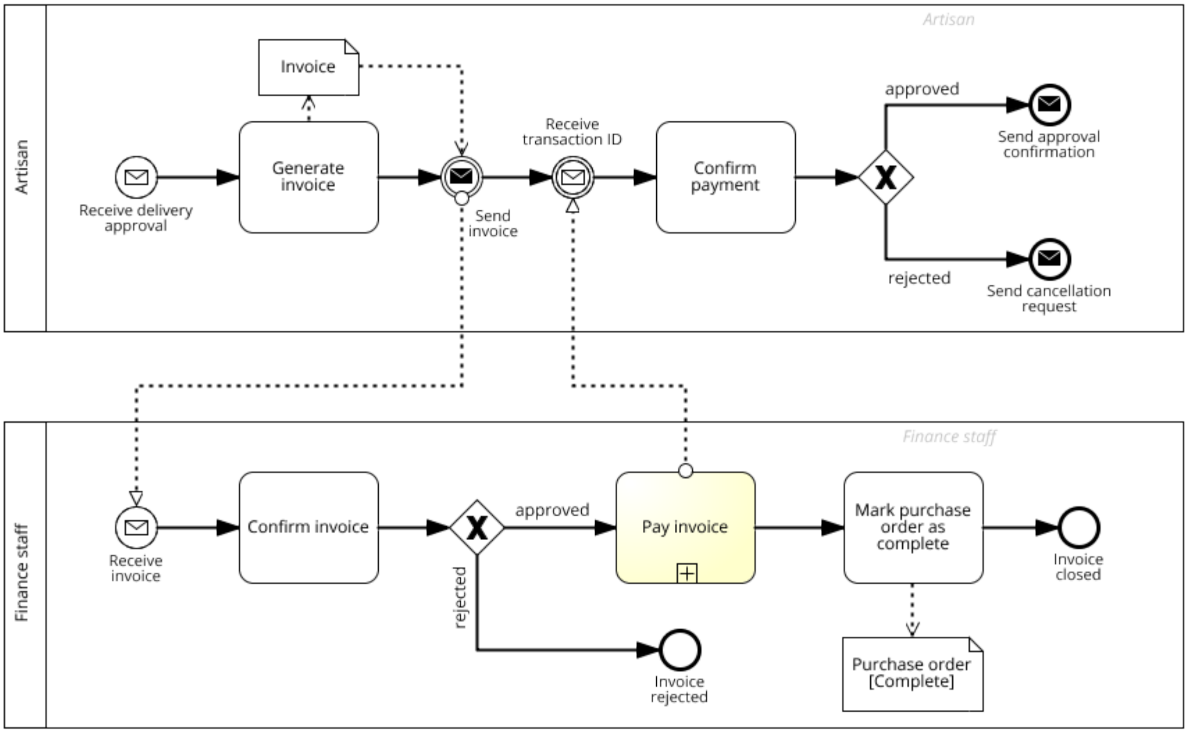


Figure 18. Process payment sub-process

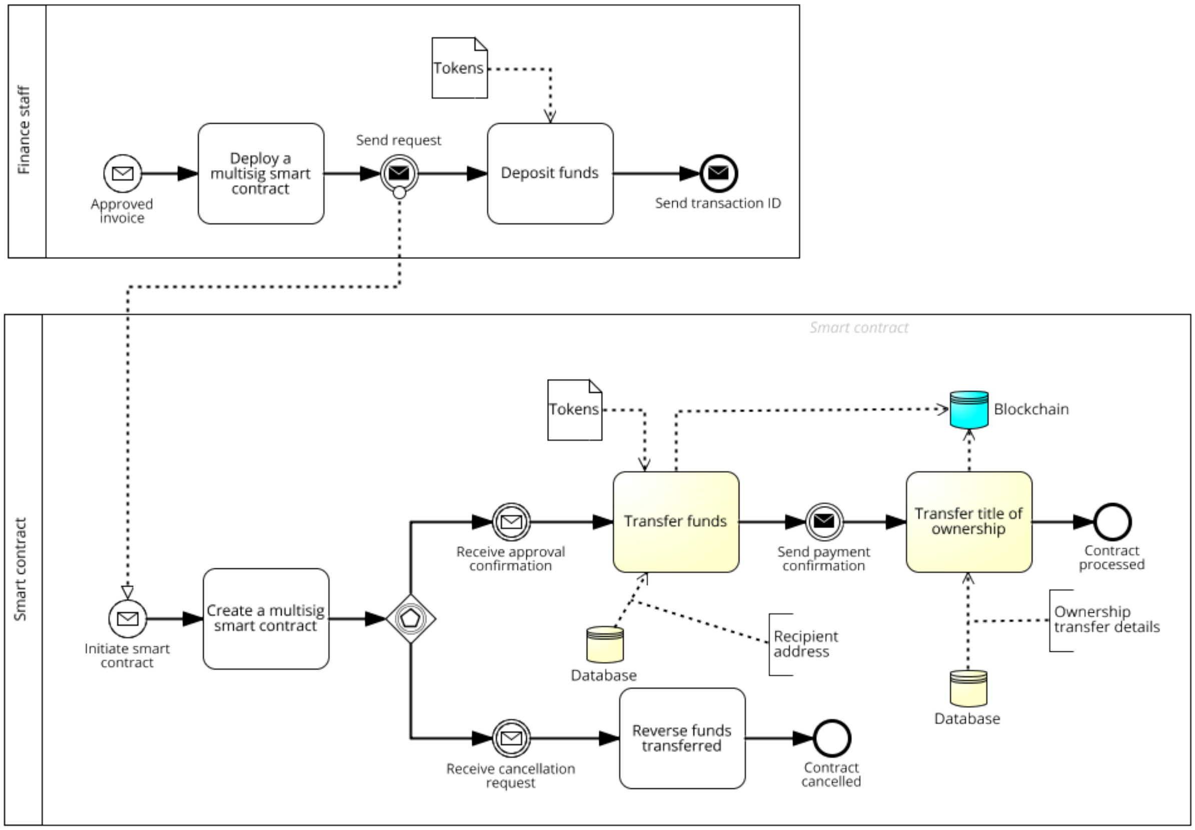


Figure 19. Pay invoice sub-process

4.5 Domain models

This section we present the domain models as UML class diagrams for the above To-Be business process model.

1. Product design model

The Product design model consist of dimensions, drawings, images, bill of materials and components. It also has a list of designers who created the product design.

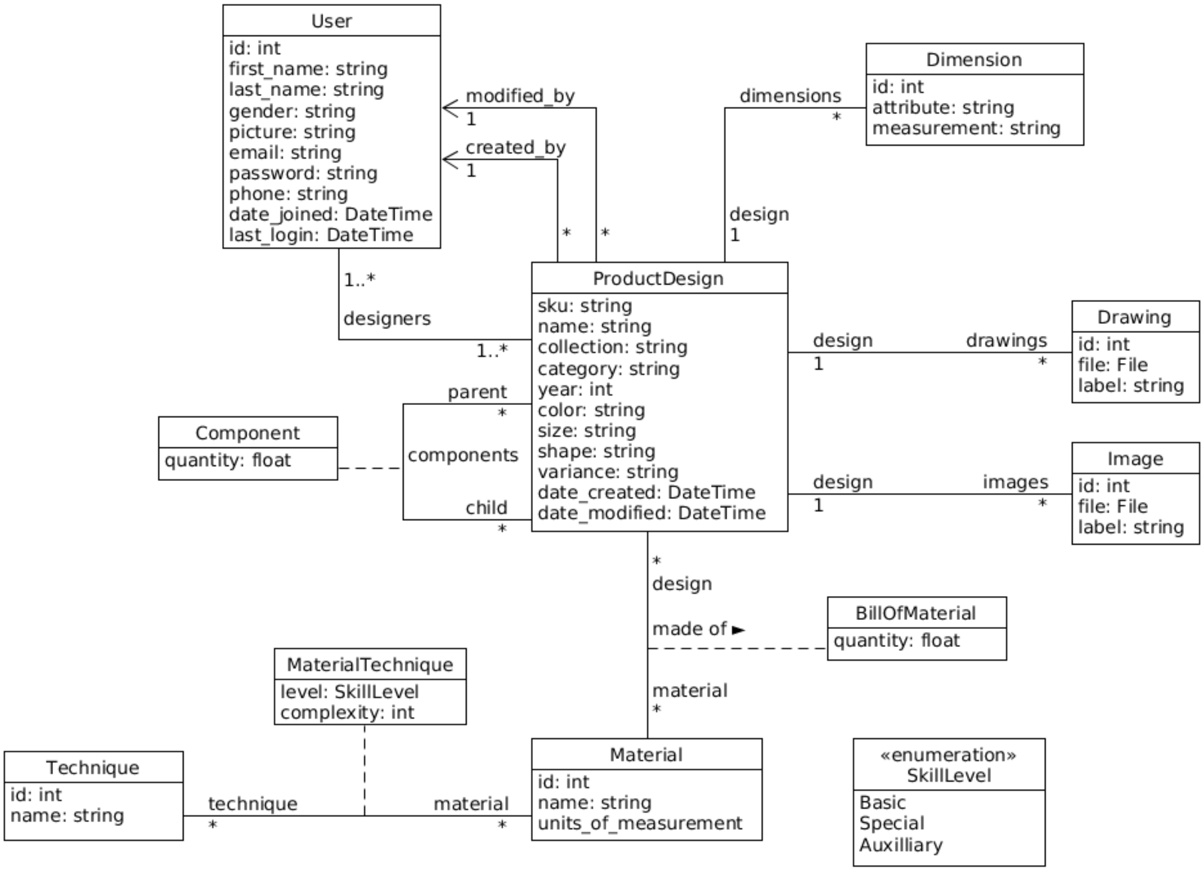


Figure 20. Product design domain model

2. Artisan production

The Artisan Production model has a one to one relationship to a Purchase Order Product and contains a list of raw materials including their sources. It also has the production location and period.

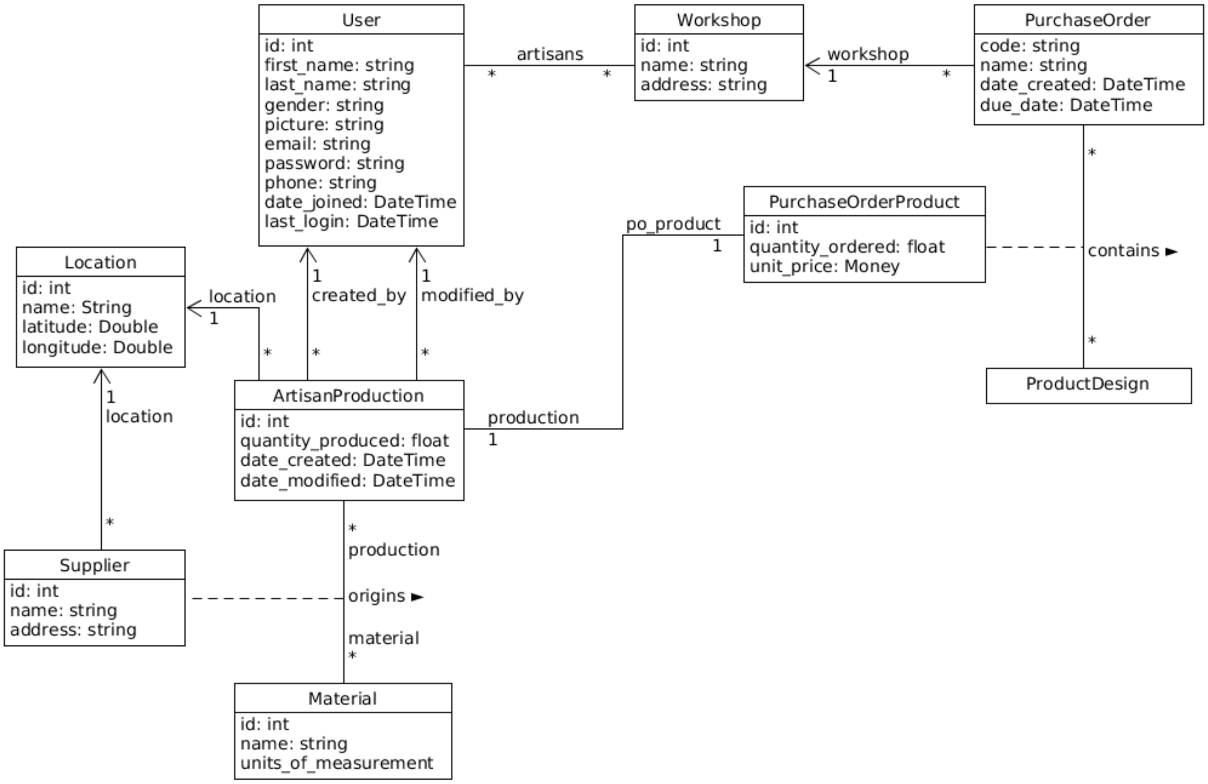


Figure 21. Artisan production domain model

3. Purchase order delivery

Items produced by an artisan ready for delivery are serialized and recorded in a Purchase Order Delivery record which acts as a handover document between the artisan and the organization (Soko).

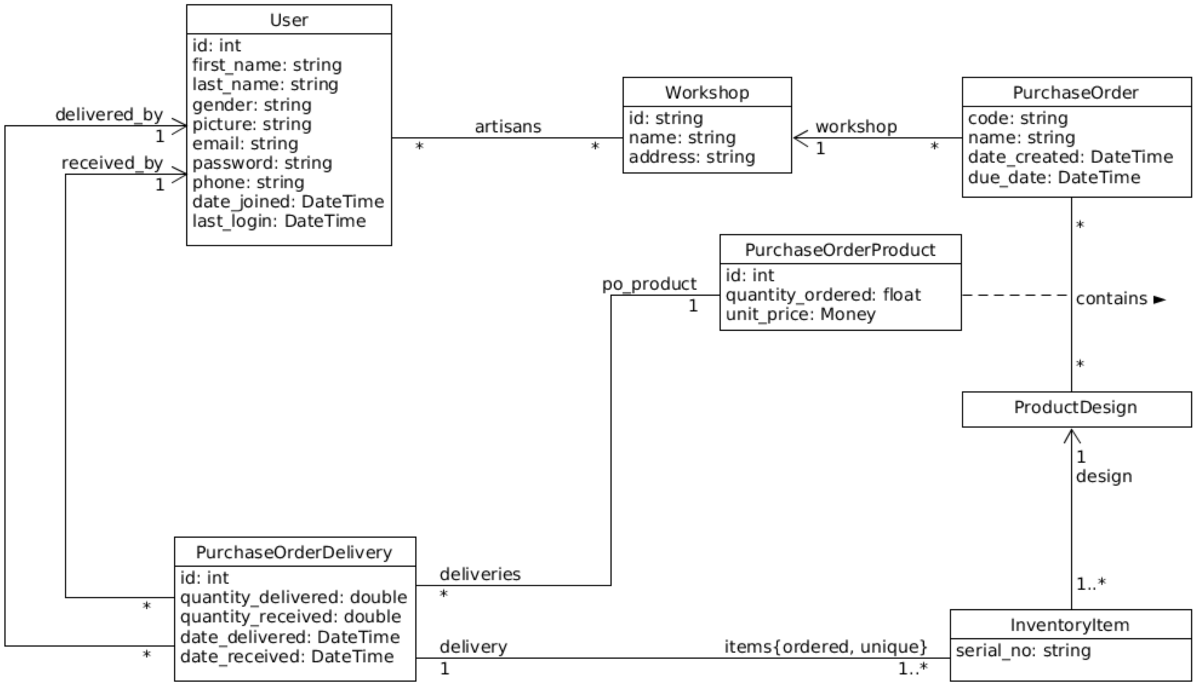


Figure 22. Purchase order delivery domain model

4. Artisan production and Work in progress validation

Validation of products from an Artisan production or Work in progress is performed at a granular level by a QA staff. This is because items from these processes are entered into the inventory as serialized items with relations to Purchase Order Delivery, Product Design and Validation records. The validation model supports both Artisan Production and In-house WIP validation stages.

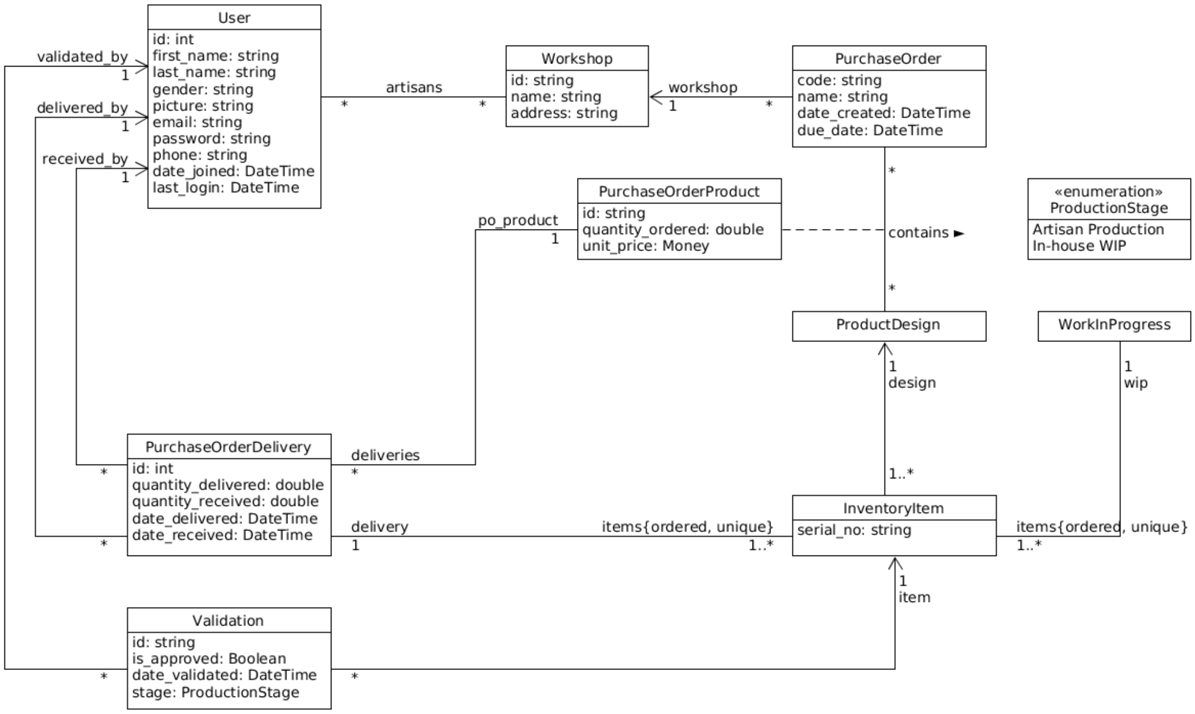


Figure 23. Validation domain model

5. Work in progress

Work in progress (WIP) is a value addition process that involves electroplating, modification and assembly sub-processes. Items received from an artisan's inhouse or external production have to undergo a value addition process so as to fit the required level of quality. Figure 24 below shows Work In Progress and its relations.

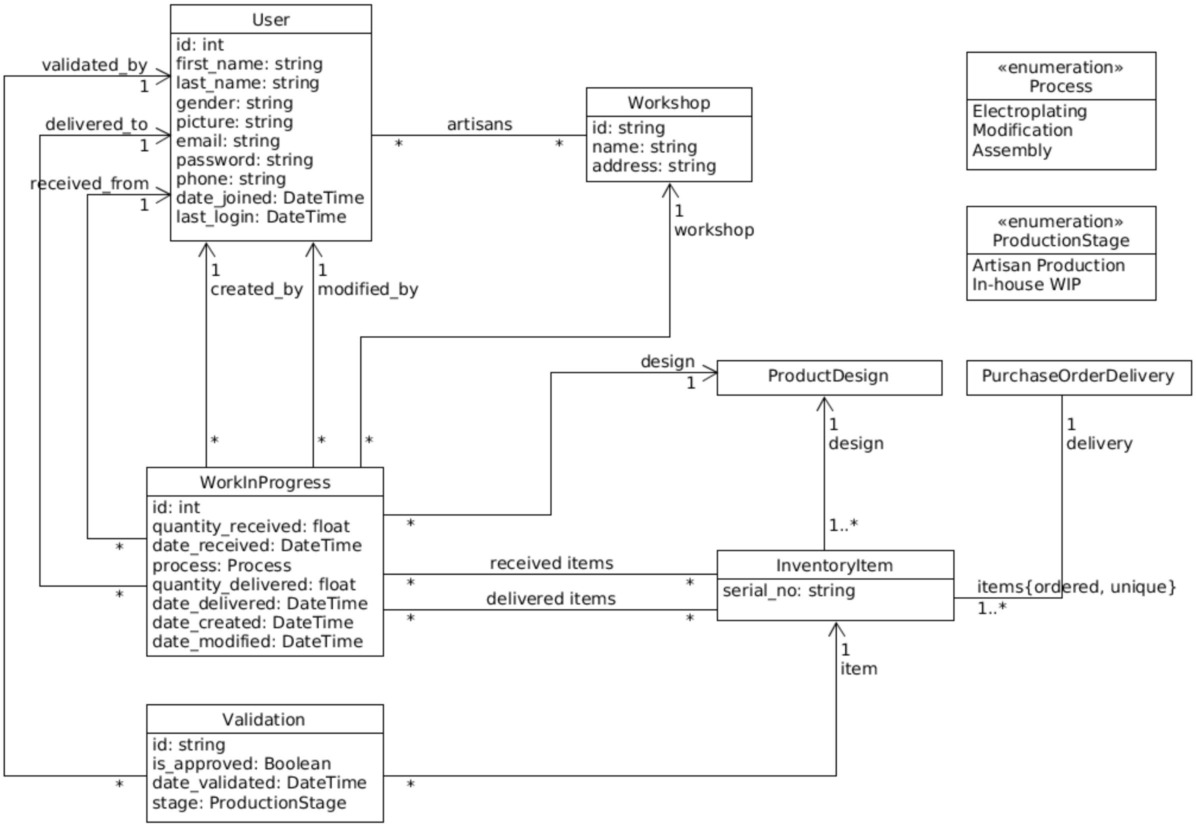


Figure 24. Work in progress domain model

6. Ownership transfer

To transfer the ownership of an item from one user to another, the Ownership Transfer model is created once a purchase order related to the production item is paid.

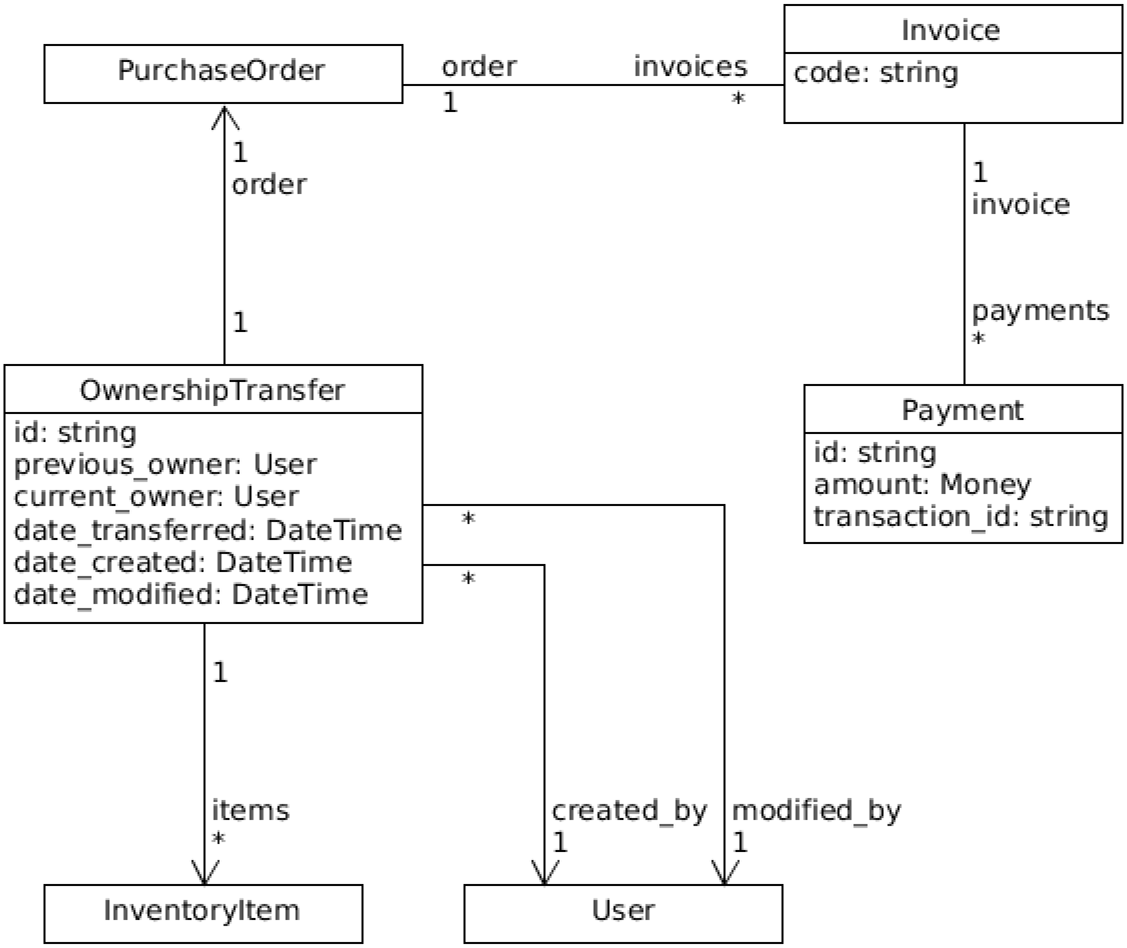


Figure 25. Ownership transfer domain model

5 Implementation

In this section, we present an architectural design for both front-end and back-end systems. The aim of this section is to provide a proof of concept on how to implement the proposed provenance solution for a handcrafted jewellery business process.

5.1 Architecture

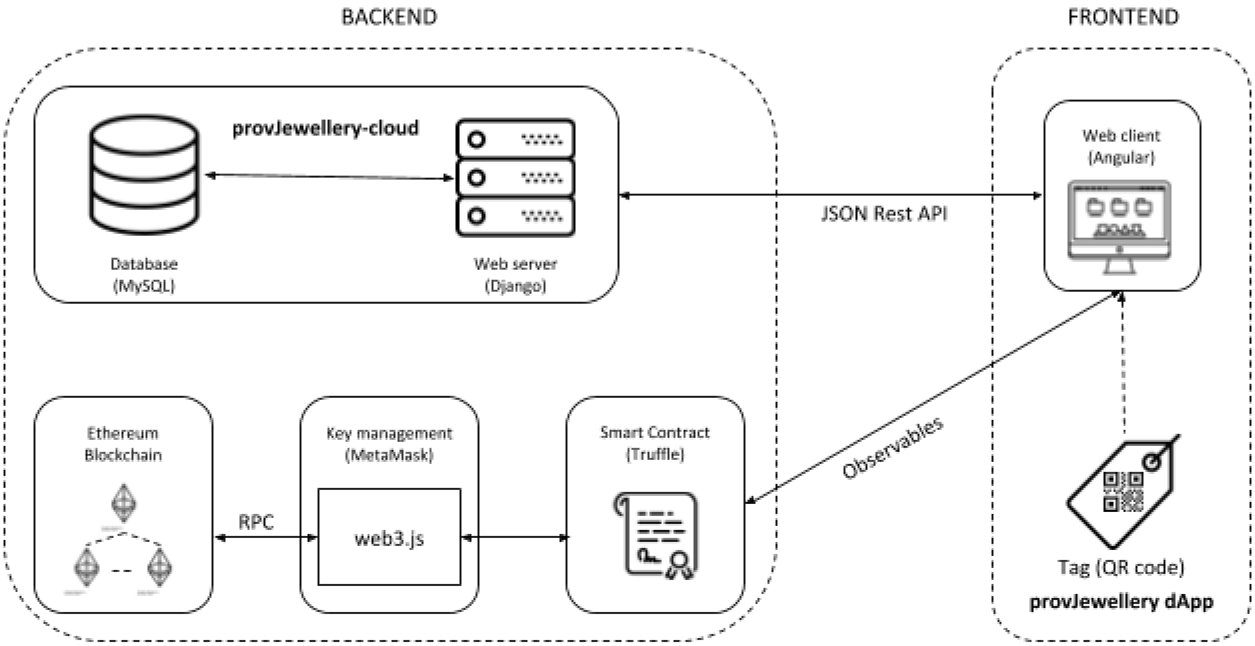


Figure 26. Architecture of the provJewellery decentralized application

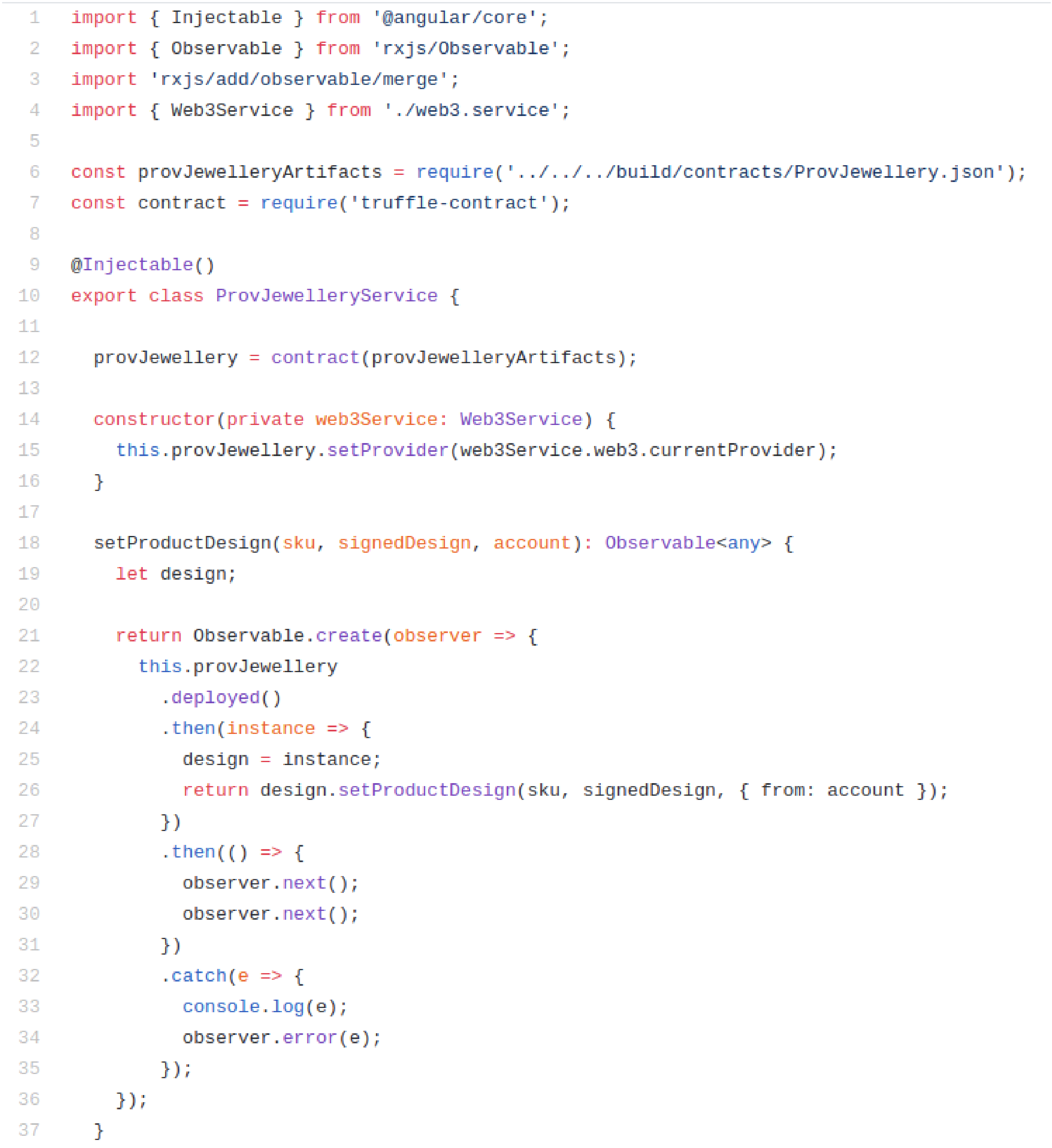
This application is called provJewellery - a provenance decentralized application (dApp) for handcrafted jewellery. The front-end consists mainly of a single page application and a tagging mechanism. The back-end system consists of a web server, a relational database, and an Ethereum node running a smart contract.

5.1.1 Front-end system

The front-end application, known as **provJewellery**[20], is written in TypeScript[21] using Angular[22] framework. TypeScript is strict syntactical superset of JavaScript that runs on most browsers in a compiled JavaScript format. Angular is a single page application development framework that is written in TypeScript and supports fast bootstrapping of an app using Angular CLI[23]. Bootstrapping in this context refers to utilising code segments generated by a software as the base of writing or running an application.

The app mainly consists of modules, components, services and routes. Components form the base micro-apps and are grouped into modules. Services allow the components to share state and make requests to the back-end via a JSON ReSTful Application Programming Interface (API). Figure 27 below shows a segment of prov-jewellery service that communicates with the web3 service to access a smart contract.

[20] https://github.com/antorenge/provJewellery
[21] https://www.typescriptlang.org/
[22] https://angular.io/
[23] https://cli.angular.io/



```
import { Injectable } from '@angular/core';
import { Observable } from 'rxjs/Observable';
import 'rxjs/add/observable/merge';
import { Web3Service } from './web3.service';

const provJewelleryArtifacts = require('../../../build/contracts/ProvJewellery.json');
const contract = require('truffle-contract');

@Injectable()
export class ProvJewelleryService {

  provJewellery = contract(provJewelleryArtifacts);

  constructor(private web3Service: Web3Service) {
    this.provJewellery.setProvider(web3Service.web3.currentProvider);
  }

  setProductDesign(sku, signedDesign, account): Observable<any> {
    let design;

    return Observable.create(observer => {
      this.provJewellery
        .deployed()
        .then(instance => {
          design = instance;
          return design.setProductDesign(sku, signedDesign, { from: account });
        })
        .then(() => {
          observer.next();
          observer.next();
        })
        .catch(e => {
          console.log(e);
          observer.error(e);
        });
    });
  }
```

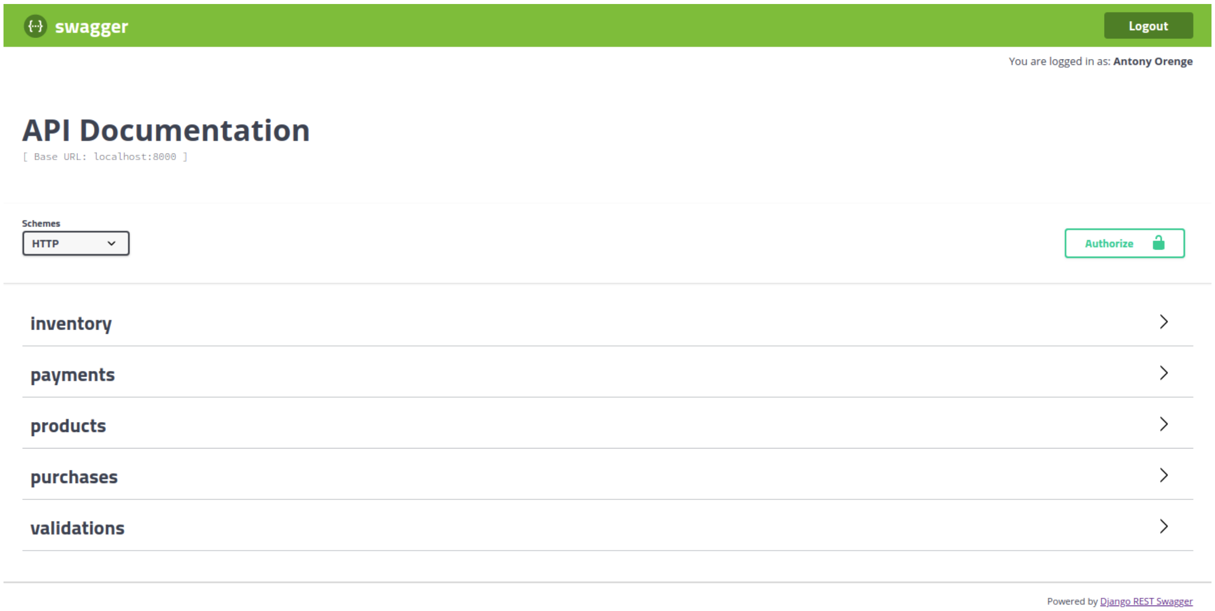
Figure 27. Code segment of prov-jewellery service file

Since, this application is primary compiled to JavaScript language, it can run on most popular web browsers. To deploy the app in a production environment, *ng build --prod* command is used to compile it into an output directory that can be served by a web server.

Tagging of items is achieved by use of QR codes. These are generated by the system based on an item's serial number. Scanning the QR code should display a link to a specific item search results on provJewellery search page.

5.1.2 Back-end system

The back-end system comprises of two main services - web and Ethereum service. The web service is known as **provJewellery-cloud**[24], which handles the business logic as per the To-Be handcrafted jewellery process flow (see section 4.4), and communicates to a MySQL[25] relational database. It is primarily written in Django 2[26] - a python 3[27] web framework that supports fast bootstrapping. To provide a JSON Rest API for communicating with the front-end, we use django rest framework[28] (DRF) package, and django rest swagger[29] for generating API documentation (see Figure 28).



You are logged in as: Antony Orenge

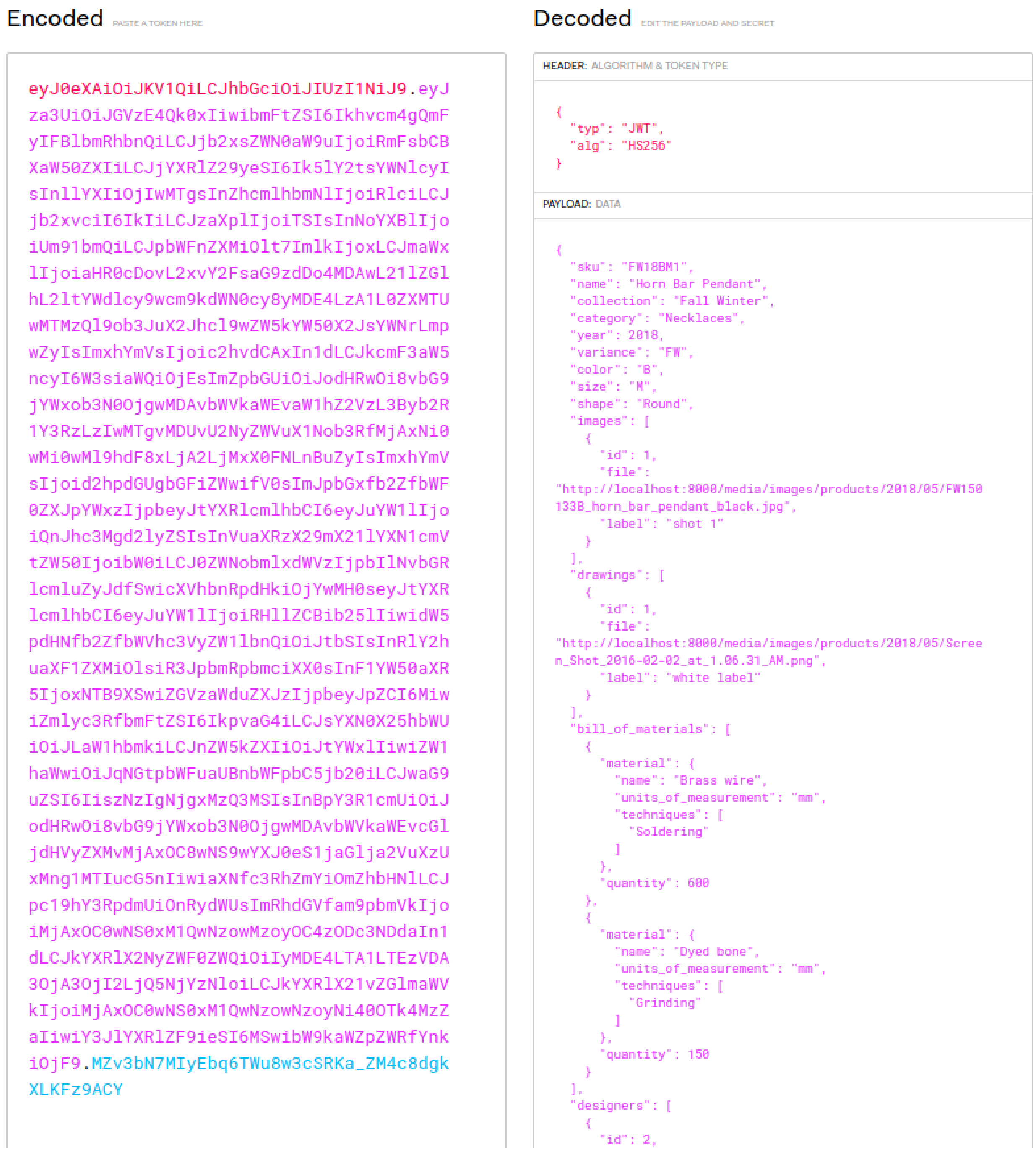
[Base URL: localhost:8000]

Figure 28. Web service API documentation

[24] https://github.com/antorenge/prov-jewellery-cloud
[25] https://www.mysql.com/
[26] https://www.djangoproject.com/
[27] https://docs.python.org/3/
[28] http://www.django-rest-framework.org/
[29] https://django-rest-swagger.readthedocs.io/en/latest/

In order to ensure secure transmission of data, we use JSON web token (JWT) - a RFC 7519[30] industry standard for representing claims between two parties. A well formed JWT consists of three strings separated by dots - a header, payload and a signature. In this implementation, Hash-Based Message Authentication Codes (HMAC)[31] and Secure Hash Algorithm (SHA256)[32] is combined to form a HS256 algorithm, which is used to cryptographically hash JSON objects by use of a shared key (Secret). The generated JWT's are digitally signed and verified by a smart contract on an Ethereum node. Figure 29 below show an encoded and decoded version of a JSON web token used in this application. The tool used in displaying this is on https://jwt.io/.

[30] https://tools.ietf.org/html/rfc7519
[31] https://en.wikipedia.org/wiki/HMAC
[32] https://en.wikipedia.org/wiki/SHA-2


Encoded PASTE A TOKEN HERE
Decoded EDIT THE PAYLOAD AND SECRET
HEADER: ALGORITHM & TOKEN TYPE
PAYLOAD: DATA

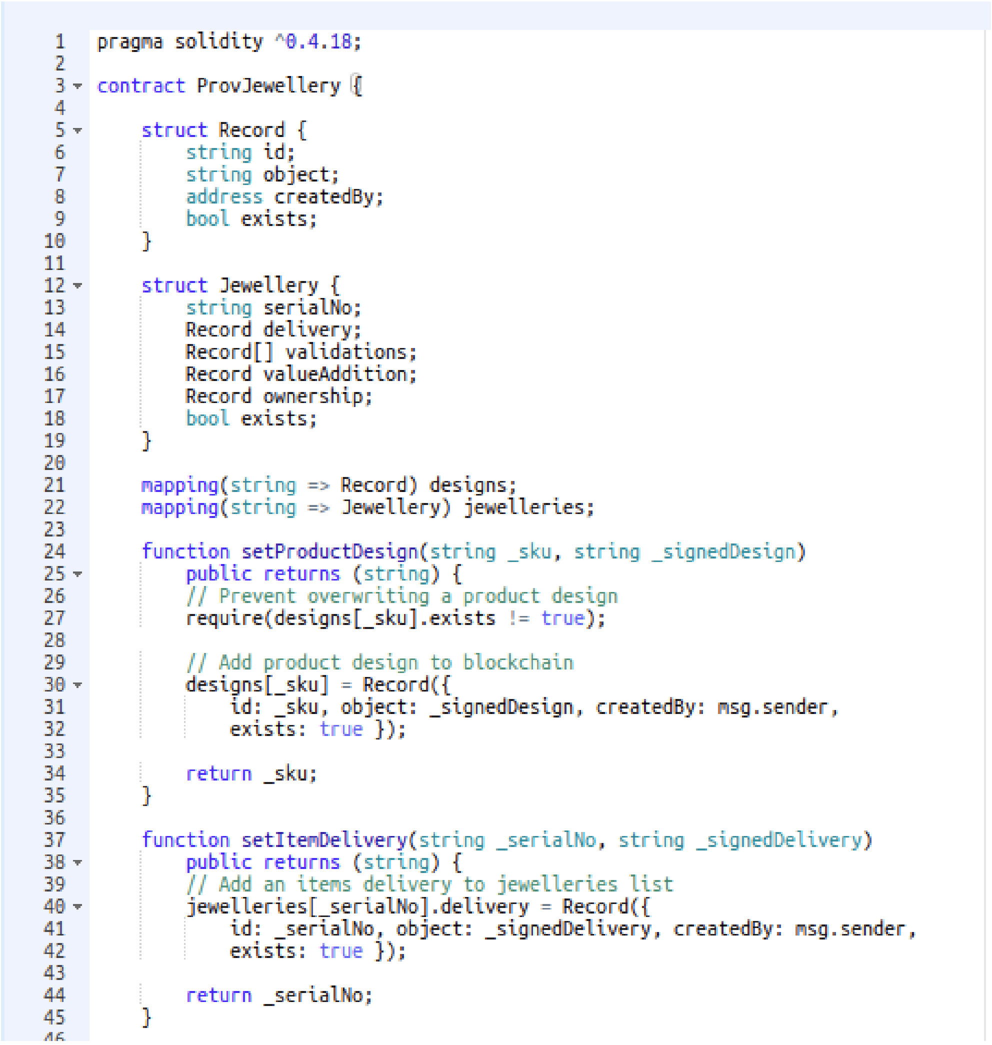
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ
za3UiOiJGVzE4Qk0xIiwibmFtZSI6Ikhvcm4gQmF
yIFBlbmRhbnQiLCJjb2xsZWN0aW9uIjoiRmFsbCB
XaW50ZXIiLCJjYXRlZ29yeSI6Ik5lY2tsYWNlcyI
sInllYXIiOjIwMTgsInZhcmlhbmNlIjoiRlciLCJ
jb2xvciI6IkIiLCJzaXplIjoiTSIsInNoYXBlIjo
iUm91bmQiLCJpbWFnZXMiOlt7ImlkIjoxLCJmaWx
lIjoiaHR0cDovL2xvY2FsaG9zdDo4MDAwL21lZGl
hL2ltYWdlcy9wcm9kdWN0cy8yMDE4LzA1L0ZXMTU
wMTMzQl9ob3JuX2Jhcl9wZW5kYW50X2JsYWNrLmp
wZyIsImxhYmVsIjoic2hvdCAxIn1dLCJkcmF3aW5
ncyI6W3siaWQiOjEsImZpbGUiOiJodHRwOi8vbG9
jYWxob3N0OjgwMDAvbWVkaWEvaW1hZ2VzL3Byb2R
1Y3RzLzIwMTgvMDUvU2NyZWVuX1Nob3RfMjAxNi0
wMi0wMl9hdF8xLjA2LjMxX0FNLnBuZyIsImxhYmV
sIjoid2hpdGUgbGFiZWwifV0sImJpbGxfb2ZfbWF
0ZXJpYWxzIjpbeyJtYXRlcmlhbCI6eyJuYW1lIjo
iQnJhc3Mgd2lyZSIsInVuaXRzX29mX21lYXN1cmV
tZW50IjoibW0iLCJ0ZWNobmlxdWVzIjpbIlNvbGR
lcmluZyJdfSwicXVhbnRpdHkiOjYwMH0seyJtYXR
lcmlhbCI6eyJuYW1lIjoiRHllZCBib25lIiwidW5
pdHNfb2ZfbWVhc3VyZW1lbnQiOiJtbSIsInRlY2h
uaXF1ZXMiOlsiR3JpbmRpbmciXX0sInF1YW50aXR
5IjoxNTB9XSwiZGVzaWduZXJzIjpbeyJpZCI6Miw
iZmlyc3RfbmFtZSI6IkpvaG4iLCJsYXN0X25hbWU
iOiJLaW1hbmkiLCJnZW5kZXIiOiJtYWxlIiwiZW1
haWwiOiJqNGtpbWFuaUBnbWFpbC5jb20iLCJwaG9
uZSI6IiszNzIgNjgxMzQ3MSIsInBpY3R1cmUiOiJ
odHRwOi8vbG9jYWxob3N0OjgwMDAvbWVkaWEvcGl
jdHVyZXMvMjAxOC8wNS9wYXJ0eS1jaGlja2VuXzU
xMng1MTIucG5nIiwiaXNfc3RhZmYiOmZhbHNlLCJ
pc19hY3RpdmUiOnRydWUsImRhdGVfam9pbmVkIjo
iMjAxOC0wNS0xM1QwNzowMzoyOC4zODc3NDdaIn1
dLCJkYXRlX2NyZWF0ZWQiOiIyMDE4LTA1LTEzVDA
3OjA3OjI2LjQ5NjYzNloiLCJkYXRlX21vZGlmaWV
kIjoiMjAxOC0wNS0xM1QwNzowNzoyNi40OTk4MzZ
aIiwiY3JlYXRlZF9ieSI6MSwibW9kaWZpZWRfYnk
iOjF9.MZv3bN7MIyEbq6TWu8w3cSRKa_ZM4c8dgk
XLKFz9ACY
```

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

```
{
  "sku": "FW18BM1",
  "name": "Horn Bar Pendant",
  "collection": "Fall Winter",
  "category": "Necklaces",
  "year": 2018,
  "variance": "FW",
  "color": "B",
  "size": "M",
  "shape": "Round",
  "images": [
    {
      "id": 1,
      "file":
"http://localhost:8000/media/images/products/2018/05/FW150
133B_horn_bar_pendant_black.jpg",
      "label": "shot 1"
    }
  ],
  "drawings": [
    {
      "id": 1,
      "file":
"http://localhost:8000/media/images/products/2018/05/Scree
n_Shot_2016-02-02_at_1.06.31_AM.png",
      "label": "white label"
    }
  ],
  "bill_of_materials": [
    {
      "material": {
        "name": "Brass wire",
        "units_of_measurement": "mm",
        "techniques": [
          "Soldering"
        ]
      },
      "quantity": 600
    },
    {
      "material": {
        "name": "Dyed bone",
        "units_of_measurement": "mm",
        "techniques": [
          "Grinding"
        ]
      },
      "quantity": 150
    }
  ],
  "designers": [
    {
      "id": 2,
```

Figure 29. Sample encoded and decoded JWT

The Ethereum service comprise of smart contracts that can be accessed via an Application Binary Interface (ABI). ReactiveX[33] (RxJS), a reactive programming library that makes it easier to support asynchronous or callback-based code, is integrated with Truffle[34] framework to enable the front-end app to asynchronously communicate with the smart contracts via an ABI. Truffle is a JavaScript framework that supports compiling, linking, deploying and binary management of smart contracts. Figure 30 below shows a code segment of ProvJewellery smart contract.



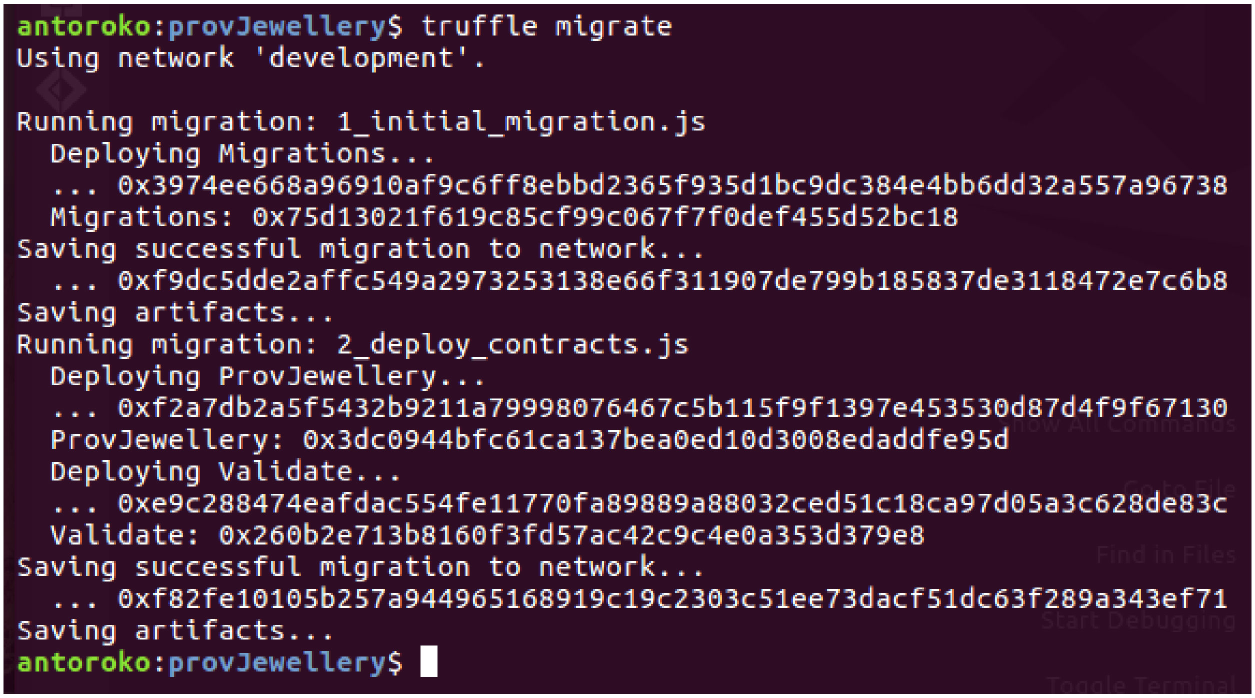
```
pragma solidity ^0.4.18;

contract ProvJewellery {

    struct Record {
        string id;
        string object;
        address createdBy;
        bool exists;
    }

    struct Jewellery {
        string serialNo;
        Record delivery;
        Record[] validations;
        Record valueAddition;
        Record ownership;
        bool exists;
    }

    mapping(string => Record) designs;
    mapping(string => Jewellery) jewelleries;

    function setProductDesign(string _sku, string _signedDesign)
        public returns (string) {
        // Prevent overwriting a product design
        require(designs[_sku].exists != true);

        // Add product design to blockchain
        designs[_sku] = Record({
            id: _sku, object: _signedDesign, createdBy: msg.sender,
            exists: true });

        return _sku;
    }

    function setItemDelivery(string _serialNo, string _signedDelivery)
        public returns (string) {
        // Add an items delivery to jewelleries list
        jewelleries[_serialNo].delivery = Record({
            id: _serialNo, object: _signedDelivery, createdBy: msg.sender,
            exists: true });

        return _serialNo;
    }
```

Figure 30. Solidity code segment of ProvJewellery smart contract

[33] http://reactivex.io/rxjs/

[34] http://truffleframework.com/

Smart contracts are written in Solidity language - a statically typed compiled language that runs on Ethereum Virtual Machine (EVM). Testing of smart contracts on the development environment is made possible by use of Test RPC. This is a light Remote Procedure Call server written in Node.js[35] and runs on an Ethereum private network - in this case localhost:8545. Truffle framework provides commands for compiling and deploying contracts to the Ethereum development network as shown below:



```
antoroko:provJewellery$ truffle migrate
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ... 0x3974ee668a96910af9c6ff8ebbd2365f935d1bc9dc384e4bb6dd32a557a96738
  Migrations: 0x75d13021f619c85cf99c067f7f0def455d52bc18
Saving successful migration to network...
  ... 0xf9dc5dde2affc549a2973253138e66f311907de799b185837de3118472e7c6b8
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying ProvJewellery...
  ... 0xf2a7db2a5f5432b9211a79998076467c5b115f9f1397e453530d87d4f9f67130
  ProvJewellery: 0x3dc0944bfc61ca137bea0ed10d3008edaddfe95d
  Deploying Validate...
  ... 0xe9c288474eafdac554fe11770fa89889a88032ced51c18ca97d05a3c628de83c
  Validate: 0x260b2e713b8160f3fd57ac42c9c4e0a353d379e8
Saving successful migration to network...
  ... 0xf82fe10105b257a944965168919c19c2303c51ee73dacf51dc63f289a343ef71
Saving artifacts...
antoroko:provJewellery$ 
```

Figure 31. Deploying smart contracts to blockchain using truffle framework

Ethereum has a ‘gas policy’ that controls the consumption of resources, this means that each transaction to successfully store data on the blockchain, it has to pay for a gas price. Furthermore, each transaction has to indicate a sender and recipient addresses. In this case, the sender address is the currently logged in user and the recipient address is the smart contract’s address. To facilitate managing of transactions, we use MetaMask[36] plugin that allows us to access Ethereum dApps from a web browser, without the need of running an entire Ethereum

[35] https://nodejs.org/en/

[36] https://metamask.io/

node. It does this by injecting web3.js[37] into the browser, which provides an interface for read and write operations to the Ethereum blockchain. MetaMask also supports key management for users so that they can access their Ethereum wallet accounts and approve transactions.

[37] https://github.com/ethereum/web3.js/

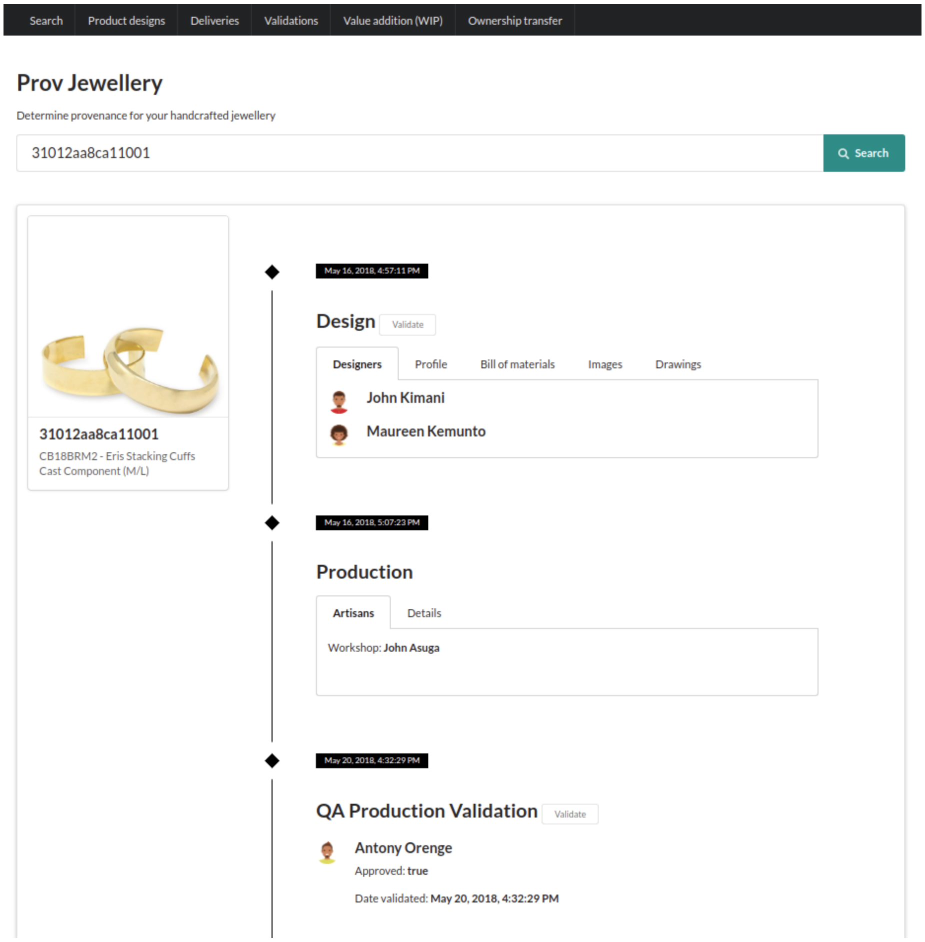
5.2 Application views

This section shows the visual interfaces for this implementation.

5.2.1 Front-end views

1. Search page view

The *search page* view is the first view when accessing the provJewellery dApp. It shows the results of a jewellery item queried from blockchain. The user has to provide a serial number. A screenshot of this page is as shown below.



Prov Jewellery

Determine provenance for your handcrafted jewellery

31012aa8ca11001

31012aa8ca11001

CB18BRM2 - Eris Stacking Cuffs Cast Component (M/L)

May 16, 2018, 4:57:11 PM

Design

John Kimani

Maureen Kemunto

May 16, 2018, 5:07:23 PM

Production

Workshop: **John Asuga**

May 20, 2018, 4:32:29 PM

QA Production Validation

Antony Orenge

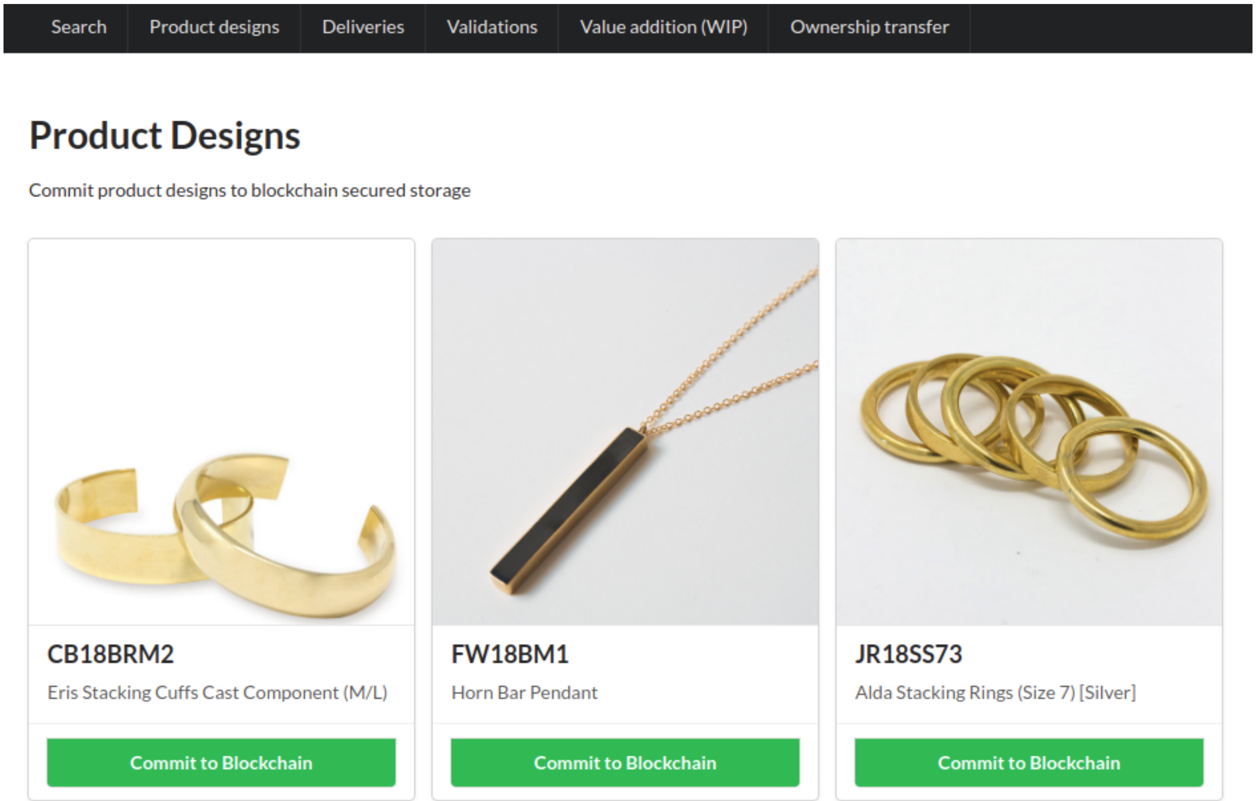
Approved: **true**

Date validated: **May 20, 2018, 4:32:29 PM**

Figure 32. ProvJewellery search page view

2. Product designs view

This view allows the designer to commit their product design record to the blockchain network. On creating a product design, the user (designer) creates a digital record of the design that includes the design profile (e.g. sku, name, color, size etc.), dimensions, images, drawings, bill of materials and a list of designers. Creation of the digital record is made possible by use of a relational model provided by the web service, the resulting JSON object is then verified by the user and the digitally signed JSON object, known as JWT, is written to the blockchain as a transaction upon clicking the commit to Blockchain button.



Product Designs

Commit product designs to blockchain secured storage

CB18BRM2
Eris Stacking Cuffs Cast Component (M/L)

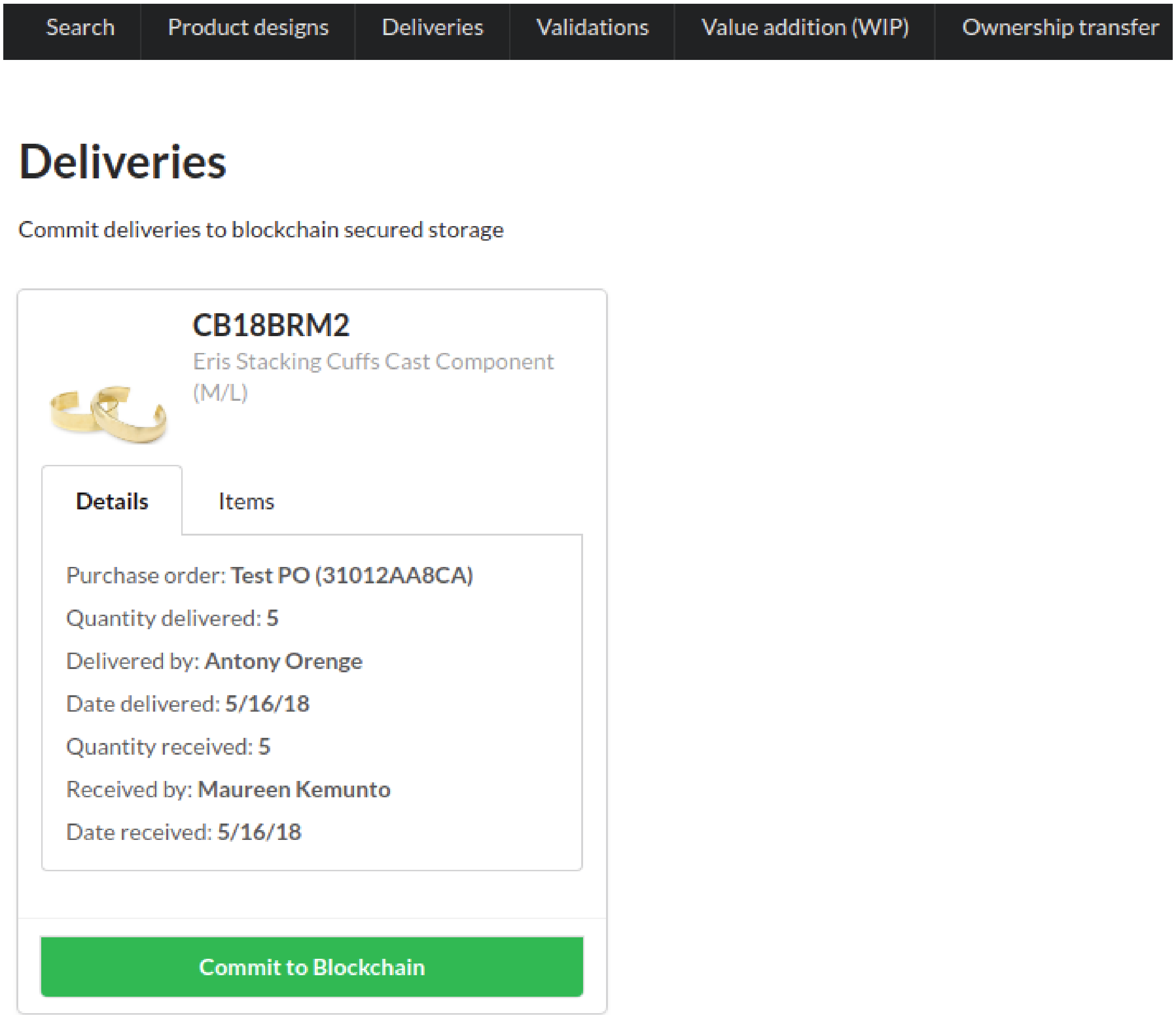
FW18BM1
Horn Bar Pendant

JR18SS73
Alda Stacking Rings (Size 7) [Silver]

Figure 33. Commit product design view

3. Deliveries view

The *deliveries view* page displays all deliveries made by an Artisan to Soko, Inc (intermediary company). A delivery shows the related purchase order, the delivery dates and handover users data. It also indicates a list of items delivered. On clicking ‘Commit to Blockchain’ button, each item is recorded on the blockchain with a copy of this delivery record.



Deliveries

Commit deliveries to blockchain secured storage

CB18BRM2

Eris Stacking Cuffs Cast Component (M/L)

Purchase order: **Test PO (31012AA8CA)**

Quantity delivered: **5**

Delivered by: **Antony Orenge**

Date delivered: **5/16/18**

Quantity received: **5**

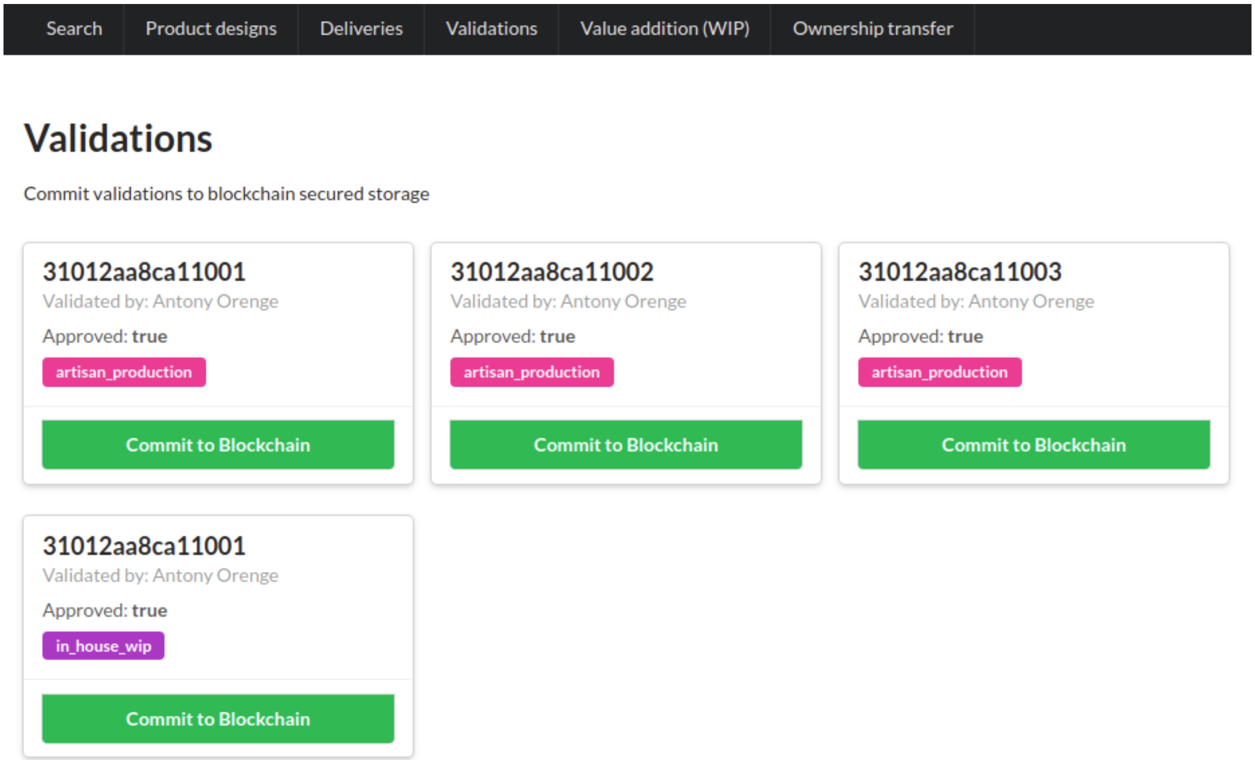
Received by: **Maureen Kemunto**

Date received: **5/16/18**

Figure 34. Deliveries view page

4. Validation view

This view displays a list of validations performed on an item. Validation details contain the item’s serial number, the QA staff that validated the item, the validation status, and the stage the item was previously from, i.e. *artisan_production* or *in_house_wip*. Clicking the commit button writes the validation result to the blockchain.



Validations

Commit validations to blockchain secured storage

31012aa8ca11001
Validated by: Antony Orenge
Approved: **true**
artisan_production

31012aa8ca11002
Validated by: Antony Orenge
Approved: **true**
artisan_production

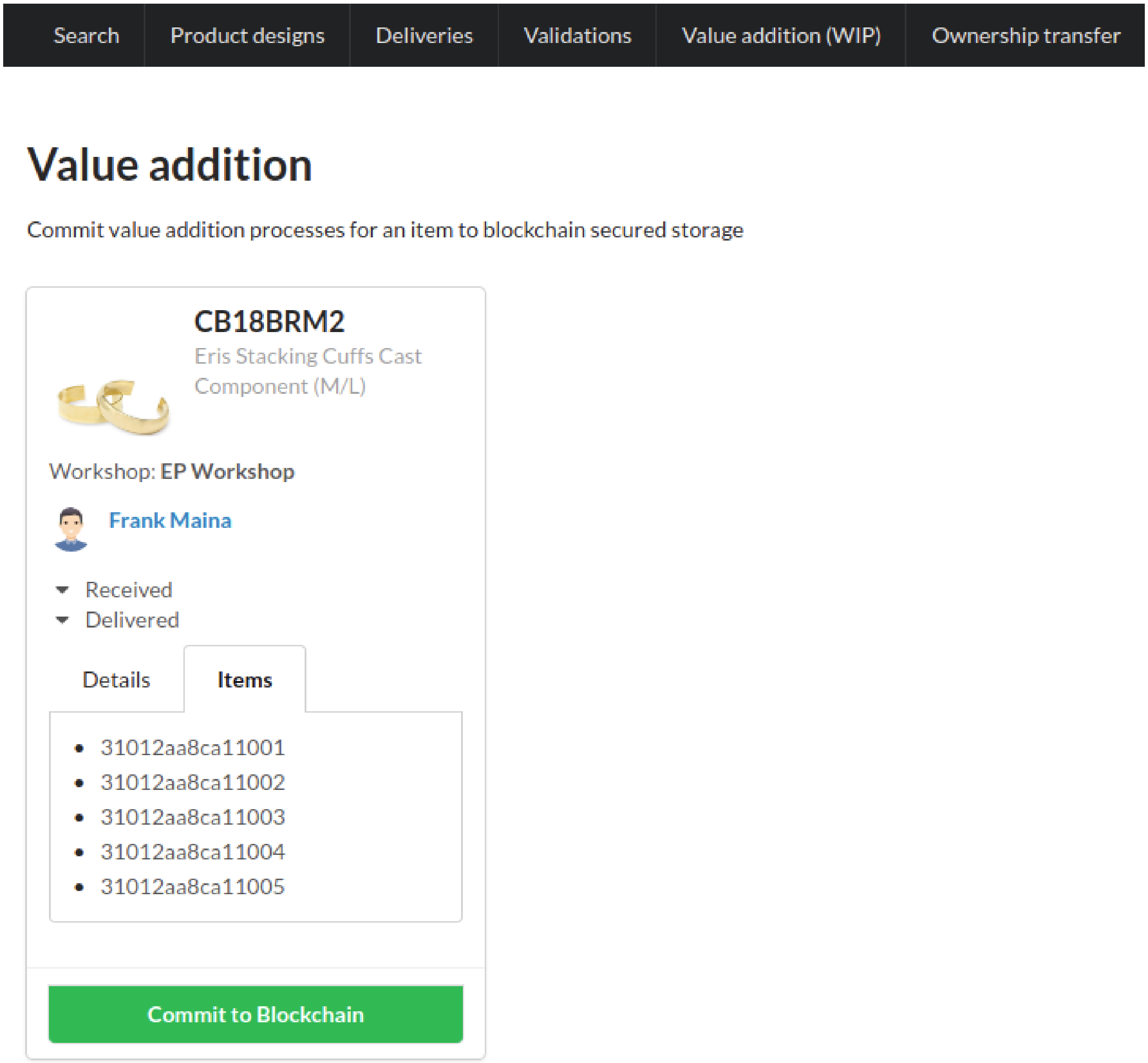
31012aa8ca11003
Validated by: Antony Orenge
Approved: **true**
artisan_production

31012aa8ca11001
Validated by: Antony Orenge
Approved: **true**
in_house_wip

Figure 35. ProvJewellery validation view

5. Value addition view

The *value addition view* page shows all the work in progress processes performed on an item so as to improve its value. The processes include electroplating, modification, and assembly. The figure below shows the value addition processes done by an in-house artisan on a list of items.



Value addition

Commit value addition processes for an item to blockchain secured storage

CB18BRM2

Eris Stacking Cuffs Cast Component (M/L)

Workshop: **EP Workshop**

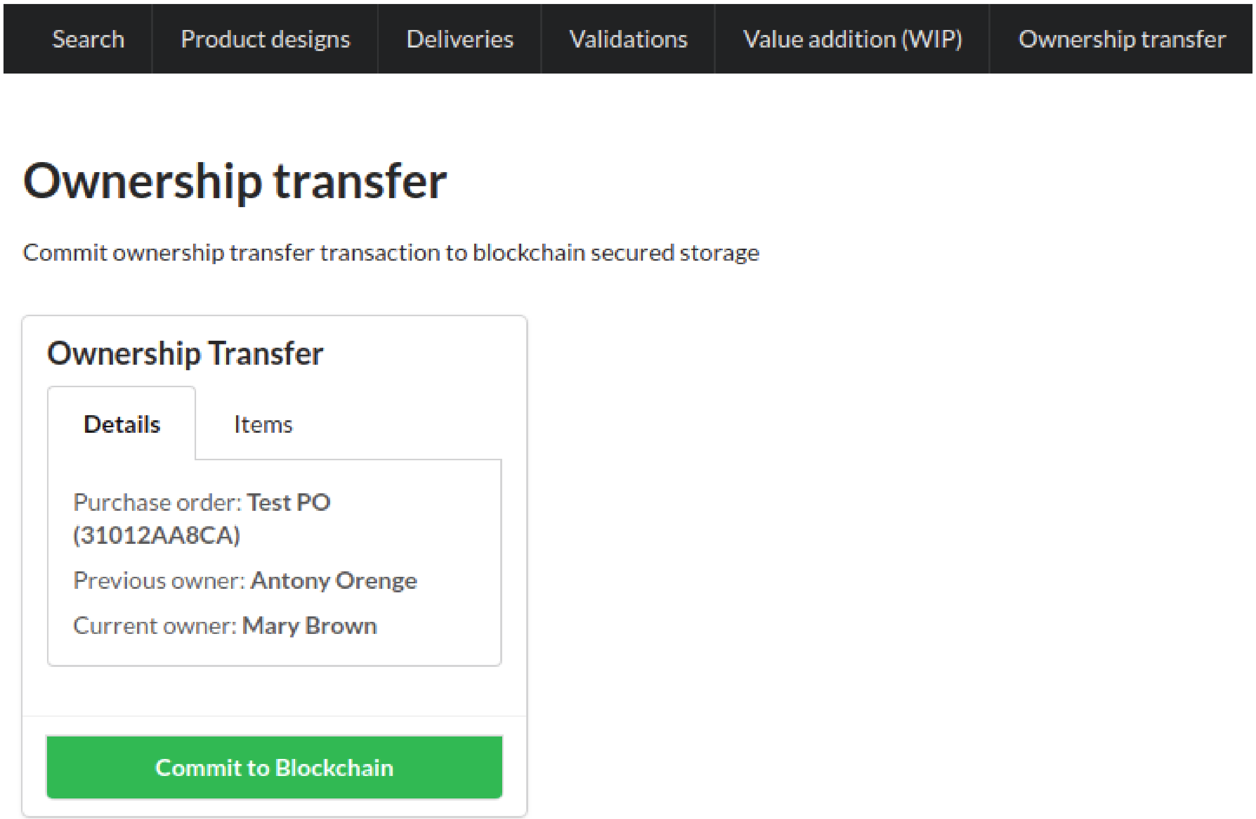
Frank Maina

- 31012aa8ca11001
- 31012aa8ca11002
- 31012aa8ca11003
- 31012aa8ca11004
- 31012aa8ca11005

Figure 36. Value addition view

6. Ownership transfer view

The *ownership transfer view* shows the exchange of claims to a jewellery piece from an artisan to the intermediary organization. Transfer of ownership if executed by the smart contract upon the artisan fulfilling a purchase and receiving payment in form of Ethereum tokens.



Commit ownership transfer transaction to blockchain secured storage

Purchase order: Test PO (31012AA8CA)

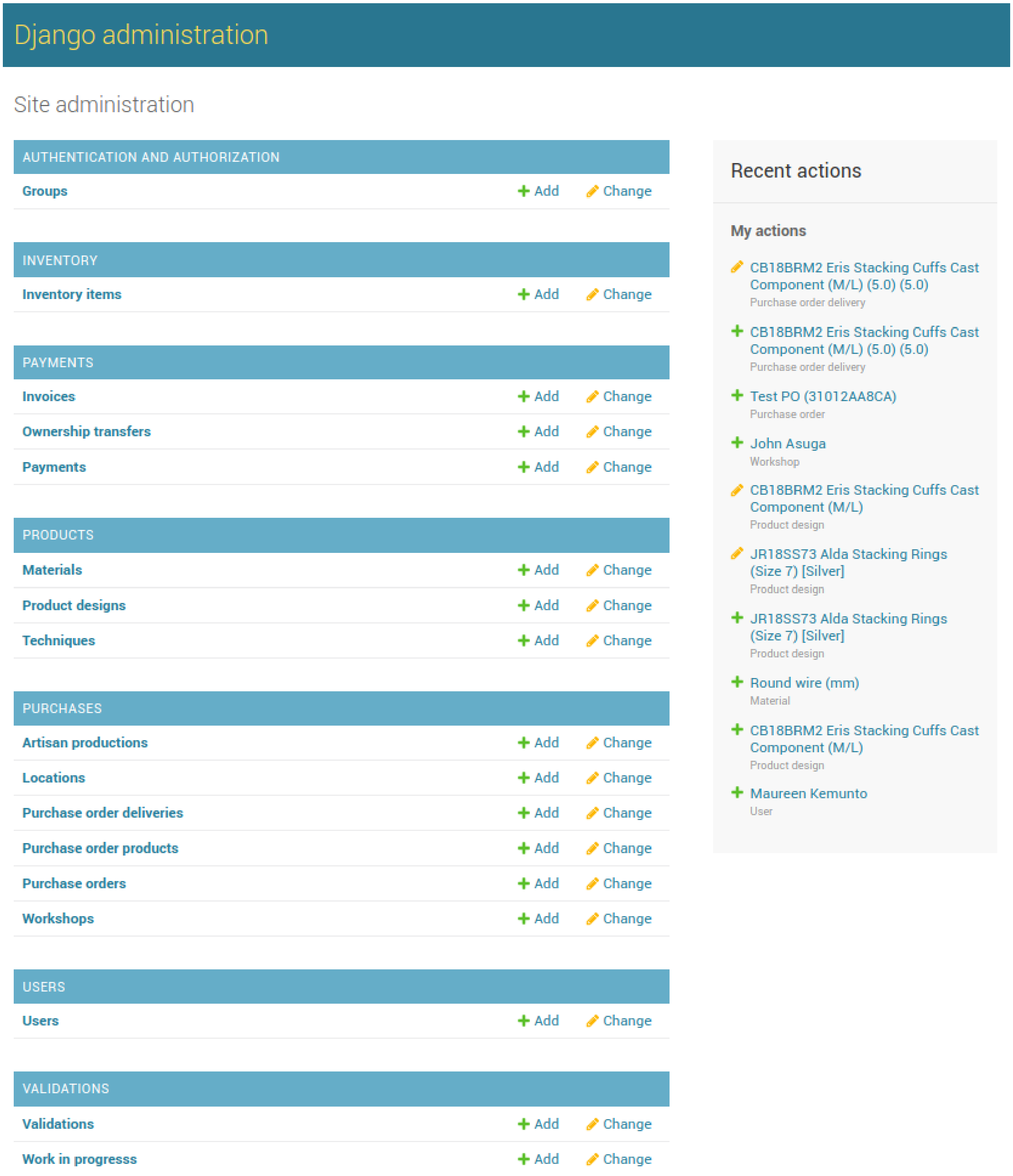
Previous owner: Antony Orenge

Current owner: Mary Brown

Figure 37. Ownership transfer view

5.2.2 Back-end view

The back-end view consists of a web service running on Django framework. The screenshot below shows all the modules implemented on the web service as per the domain models presented in Section 4.5. This service provides us with a relational model that combines with business logic to generate digital records in form of JSON objects that are signed and stored on the blockchain network.



Django administration

Site administration

AUTHENTICATION AND AUTHORIZATION		
Groups	+ Add	✎ Change

INVENTORY		
Inventory items	+ Add	✎ Change

PAYMENTS		
Invoices	+ Add	✎ Change
Ownership transfers	+ Add	✎ Change
Payments	+ Add	✎ Change

PRODUCTS		
Materials	+ Add	✎ Change
Product designs	+ Add	✎ Change
Techniques	+ Add	✎ Change

PURCHASES		
Artisan productions	+ Add	✎ Change
Locations	+ Add	✎ Change
Purchase order deliveries	+ Add	✎ Change
Purchase order products	+ Add	✎ Change
Purchase orders	+ Add	✎ Change
Workshops	+ Add	✎ Change

USERS		
Users	+ Add	✎ Change

VALIDATIONS		
Validations	+ Add	✎ Change
Work in progresss	+ Add	✎ Change

Recent actions

My actions

- ✎ CB18BRM2 Eris Stacking Cuffs Cast Component (M/L) (5.0) (5.0)
  Purchase order delivery
- + CB18BRM2 Eris Stacking Cuffs Cast Component (M/L) (5.0) (5.0)
  Purchase order delivery
- + Test PO (31012AA8CA)
  Purchase order
- + John Asuga
  Workshop
- ✎ CB18BRM2 Eris Stacking Cuffs Cast Component (M/L)
  Product design
- ✎ JR18SS73 Alda Stacking Rings (Size 7) [Silver]
  Product design
- + JR18SS73 Alda Stacking Rings (Size 7) [Silver]
  Product design
- + Round wire (mm)
  Material
- + CB18BRM2 Eris Stacking Cuffs Cast Component (M/L)
  Product design
- + Maureen Kemunto
  User

Figure 38. Django web service admin dashboard

5.3 Discussion

In this section, we discuss how the provenance features identified in section 3.5 have been factored in the above implementation. This responds to our third research questions - How to implement a provenance solution for handcrafted jewellery based on blockchain technology? We also discuss our implementation choices.

5.3.1 Metadata

The domain models presented in section 4.5 show how structural metadata relating to a handcrafted jewellery item can be modelled. For instance, the product design model (see Figure 20) has more than ten attributes such as sku, name, color, size, shape etc. These structural metadata describe how data is stored and what each piece of data means. Hence, providing a guide in designing our database schema. This can be observed from the above implementation (see section 5.1), where structural metadata is used in implementing our relational database schema, TypeScript and smart contract models. Descriptive metadata about a specific item is then added to the database, for example, Table 1 below shows multiple sku's metadata added to the product design model.

sku	name	collection	category	year	variance	color	size	shape
CB18BRM2	Eris Stacking Cuffs Cast Component (M/L)	Autumn	Bracelets	2018	CB	BR	M	Circle
FW18BM1	Horn Bar Pendant	Fall Winter	Necklaces	2018	FW	B	M	Round
JR18SS73	Alda Stacking Rings (Size 7) [Silver]	Formation	Rings	2018	JR	SS	7	Round

Table 1. Metadata of a product design

Metadata provides the primary source for establishing provenance. Thus, it has to be structured well to capture all attributes necessary to identify the target asset. In this implementation, two primary assets are targeted, i.e. product designs and jewellery items. Designs are created by designers while jewellery items are created by artisans based on the designs. Models are generated in JSON format and digitally signed into JWT strings for storing into the blockchain network. This ensures secured transmission of metadata and immutable storage on the blockchain.

5.3.2 Tagging

Tagging allows us to physically link an item to its digital record. For this reason, digital records need to have unique identifiers to link with the tags. From the to-be process design, items received from an artisan are uniquely serialized as captured by the purchase order delivery model (see Figure 22). The above implementation uses QR code technology to uniquely tag jewellery items. This allows artisans to generate QR codes as per their delivery list of serialized items (see Figure 34). Thus, a single piece of jewellery can be tracked and traced from the point it was delivered to the retail stores. Scanning QR codes provides a link which followed opens up web page that displays the history of a jewellery item from its source (see Figure 32).

5.3.3 Transparency

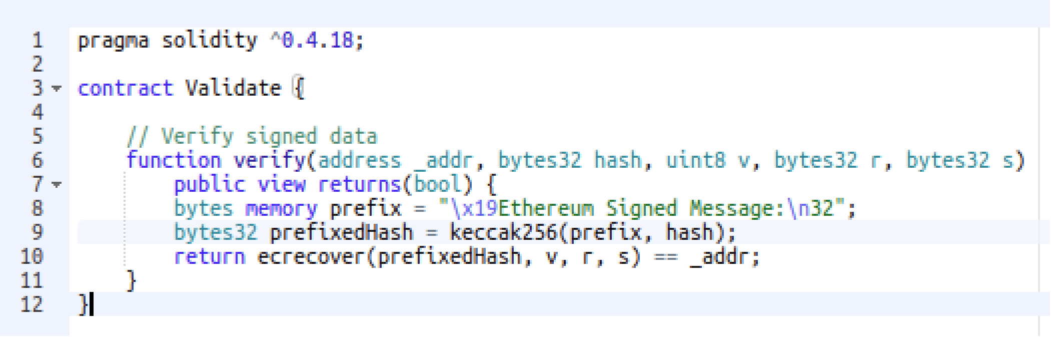
Transparency can be achieved by having information publicly accessible. Since the above solution is implemented on a public Ethereum blockchain network, any interested party can make a call to a publicly accessible smart contract address and read the provenance data. Furthermore, the above solution has a *search page view* for users to query items by their serial numbers and see their provenance data in a traceable format (see Figure 32).

5.3.4 Data verification

The proposed to-be business process model (see section 4.4) suggests the use of private and public keys for digitally signing records. These keys use the Elliptic Curve Digital Signature Algorithm (ECDSA)[38] asymmetric hashing algorithms to validate the creator of a digital signature. That is, they allow a party to sign a record using a private key and other parties can

[38] https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

use a public key to verify the record. This implies that, there can only be one user who has the private key, if not shared, and we can determine the public key of the author from the signature and verify if the digital record is the same as the one signed by the author. The figure below shows Validate contract that is used in this implementation to verify a signed record.



```
pragma solidity ^0.4.18;

contract Validate {

    // Verify signed data
    function verify(address _addr, bytes32 hash, uint8 v, bytes32 r, bytes32 s)
        public view returns(bool) {
        bytes memory prefix = "\x19Ethereum Signed Message:\n32";
        bytes32 prefixedHash = keccak256(prefix, hash);
        return ecrecover(prefixedHash, v, r, s) == _addr;
    }
}
```

Figure 39. Validate contract for data verification

To ensure secure transmission of data, we have used HS256 algorithm to cryptographically hash JSON data. This algorithm allows a party to verify data by use of a shared key, the downside been that any party with the shared key can claim ownership of the record. The reason for this implementation decision is to reduce the complexity of our proof of concept. However, for production environment, Rivest–Shamir–Adleman (RSA)[39] algorithm should be combined with ECDSA algorithm to solve this flaw.

5.3.4 Single source of truth

Single source of truth requires data to be stored exactly once. This implementation fails to fully consider this feature request. The reason is that business operations are relational in nature while the intended single source of truth storage, i.e. blockchain, does not yet fully support relational models. Hence, the need to introduce relational database in our implementation so as to construct relational models, thereafter this output in form of JSON objects is verified by the user before its equivalent cryptographically hashed value (JSON web token) is committed to the blockchain. Therefore, users can perform call operations to read data from the blockchain storage.

[39] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

6 Conclusion

This thesis proposes to design and develop a provenance solution for handcrafted jewellery by use of blockchain technology. Establishing provenance supports transparency and traceability of complex supply chains such as the handcrafted jewellery supply chain. This allows valuable handcrafted jewellery to be tracked and traced from their origins to retail stores. To achieve this, we looked into similar blockchain-based provenance solutions from different domains. We presented how they have achieved their implementation and drew key features to guide us in our design and implementation.

To model our provenance solution, we presented a case study of a handcrafted jewellery global supply chain company. We analysed their current as-is business process and identified issues hindering provenance. Thereafter, we proposed a to-be business process that guarantees provenance by use of blockchain technology. As a proof of concept we implemented our to-be business process so as to demonstrate the feasibility of our design. Thus, answering our third research question on how to implement a provenance solution for handcrafted jewellery based on blockchain technology. We further discussed on how the key features we identified for designing a provenance solution have been applied in our to-be process design and implementation.

This research opens way to more future opportunities on provenance and how to enhance this solution for handcrafted jewellery. We would like to make improvements in capturing data from the source, provide a more secure way of tagging items, implement most part of this solution onto the blockchain network, and provide an easier way for artisans to exchange digital currency for fiat currency. In addition, we would like to improve on the user interface design for the provJewellery dApp and make it freely available for consumers to download and use.

References

[1] Praxiom Research Group Limited. ISO 9000 2015. Plain English Definitions. http://www.praxiom.com/iso-definition.htm (27.04.2018)

[2] Swanson, T. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, page 4, 2015. https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf (27.04.2018)

[3] Wood, G. Ethereum: A secure decentralised generalised transaction ledger. EIP-150 Revision. http://gavwood.com/paper.pdf (15.03.2018)

[4] Delmolino, K., Arnett, M., Kosba, A., Miller, A. and Shi, E. Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. http://fc16.ifca.ai/bitcoin/papers/DAKMS16.pdf (30.03.2018)

[5] Rajaraman, V. Reson (2017) 22: 549. https://doi-org.ezproxy.utlib.ut.ee/10.1007/s12045-017-0498-6

[6] Denso Wave Incorporated. QR Code standardization. (2003). http://www.denso-wave.com/qrcode/qrstandard-e.html (27.11.2017)

[7] World Health Organization. Global and regional food consumption patterns and trends: Availability and consumption of fish. 2017. http://www.who.int/nutrition/topics/3_foodconsumption/en/index5.html (12.12.2017)

[8] Future of Fish. Making Sense of Wild Seafood Supply Chains. A report created for The Nature Conservancy. 2015. http://futureoffish.org/sites/default/files/docs/resources/TNC.SeafoodSupplyChainReport.V10.Web_.pdf (12.12.2017)

[9] Provenance.org. From shore to plate: Tracking tuna on the blockchain. 15 July 2016. https://www.provenance.org/tracking-tuna-on-the-blockchain (23.10.2017)

[10] Responsible Jewellery Council. Provenance Claims. https://www.responsiblejewellery.com/rjc-certification/code-of-practices-certification13-2/training/provenance-claims-cop-2013/ (22.02.2018)

[11] United Nations General Assembly Session 55 Resolution 56. The role of diamonds in fuelling conflict: breaking the link between the illicit transaction of rough diamonds and armed conflict as a contribution to prevention and settlement of conflicts A/RES/55/56 1 December 2000. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/55/56 (15.03.2018)

[12] Bates, R. New GIA Program Tracks Diamonds Through the Pipeline. 26 May 2017. https://www.jckonline.com/editorial-article/new-gia-program-tracks-diamonds-through-the-pipeline/ (21.02.2018)

[13] World Health Organization. Substandard and falsified medical products. 2018. http://www.who.int/mediacentre/factsheets/fs275/en/ (19.02.2018)

[14] Southwick, N Counterfeit Drugs Kill 1 Mn People Annually: Interpol. 24 October 2013. https://www.insightcrime.org/news/brief/counterfeit-drugs-kill-1-million-annually-interpol/ (27.11.2017)

[15] World Health Organization. Anti-counterfeit Technologies for the Protection of Medicines. 2007. http://www.fip.org/impactglobalforum/pdf/backgroundinfo/IMPACT%20-%20AC%20Technologies%20v2.pdf (19.02.2018)

[16] European Commission. Guidelines of 5 November 2013 on Good Distribution Practice of medicinal products for human use 2013/C 343/01. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:343:0001:0014:EN:PDF (15.03.2018)

[17] Codex Protocol. A Decentralized Title Registry and Cryptocurrency for the Arts & Collectibles Market, Whitepaper. 2018. https://www.codexprotocol.com/ (22.02.2018)

Appendix

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, Antony Oroko Orenge,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

   of my thesis

   Blockchain-based Provenance Solution for Handcrafted Jewellery,

   supervised by Luciano Garcia Banuelos and Fredrik Payman Milani,
2. I am aware of the fact that the author retains these rights.
3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, 15.05.2018