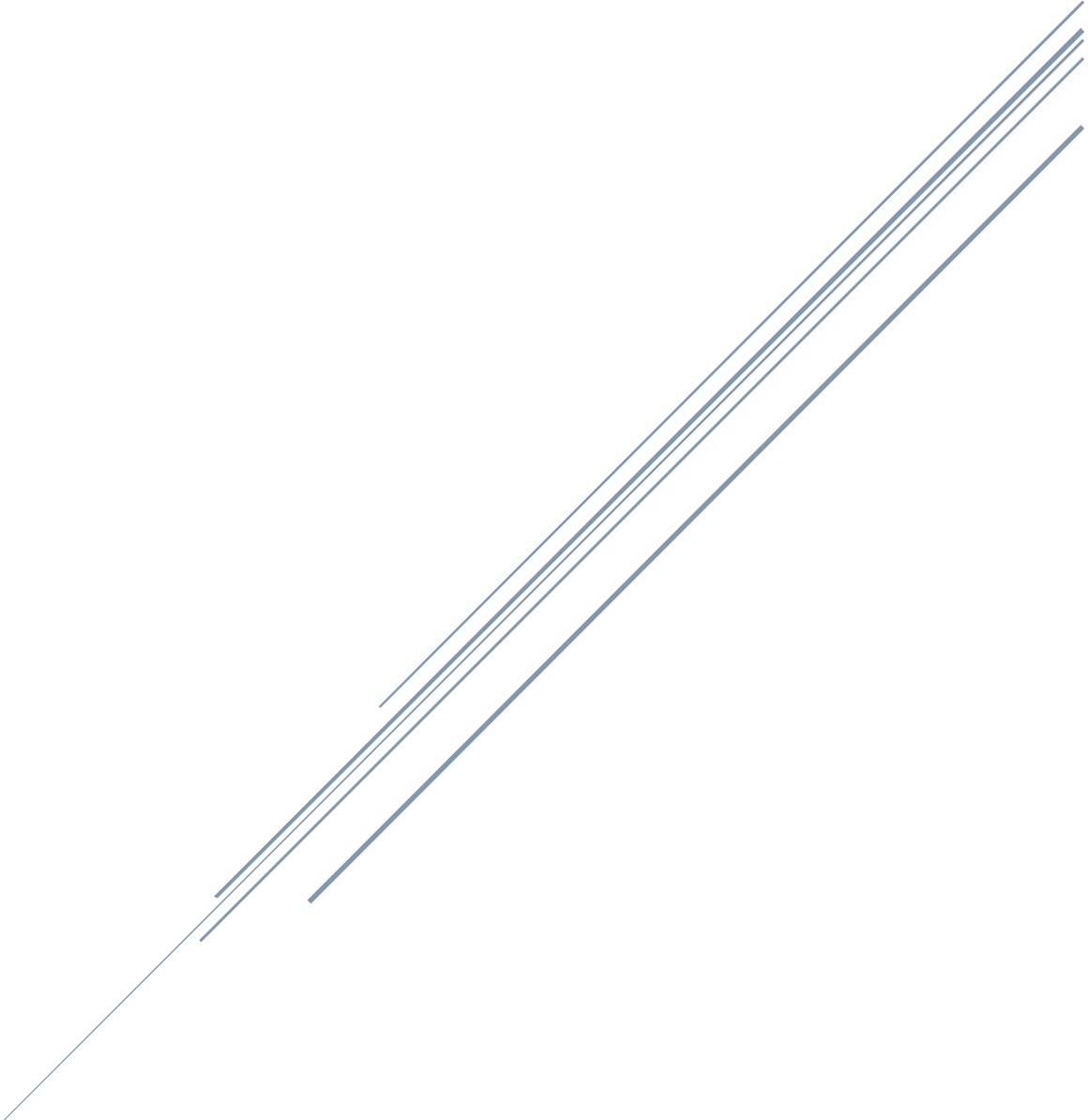


HYPERLEDGER - SUPPLY CHAIN

TRACEABILITY: ANTI COUNTERFEITING

Hyperledger Requirements Working Group



Aaron Benningfield
Blockchain Strategist

Author: Aaron Benningfield

Reviewers: Oleg Abdrashitov, Clive Boulton, Dr. Andreas Freund, Mahesh Govind.

Aaron.b.benningfield {Blockchain Strategist} @outlook.com
Oleg.a {Head of Blockchain Practice, Altos} @altoros.com
Mahesh {CEO Digiledge} @digiledge.com
Clive.boulton {DLT Specialist} @gmail.com
Andreas.freund {Head TCS Blockchain Advisory} @tcs.com

Abstract:

Blockchain's growth in Fintech will be eclipsed by the growth of Blockchain within Supply Chain. To capitalize on this growth, this foundational use case has been created to provide a foundation for enabling the myriad supply chain requirements unique to an organization to be implemented in Blockchain. This use case defines a counterfeit traceability scenario where the Blockchain capabilities would address counterfeit issues. A high level architectural flow with detailed explanation, key concepts required for driving out additional use cases and general requirements pertinent to traceability have been included to provide additional insight into the problem.

Supply Chain Traceability

Section 1 - Intro

Overview of the Business Problem or Opportunity

This use case is designed to explore supply chain traceability from the perspective of tracing counterfeit microchips being from a specific geo that indicates to the United States Customs department that the incoming microchips in review are counterfeit. Using the Hyperledger DLT to provide automated tracing, notification and other alerts, appropriate users in the Channel are quickly updated to the status of the incoming parts (microchips) and can proceed accordingly.

This use case presents a simpler routing and exercise of supply chain traceability in that there are five actors involved within the channel with one playing in a criminal role and one ethically “challenged” if not quite legally complicit. Due to the vast array of what organizations consider their supply chain, the sophistication and pure supply chain permutations make it difficult to provide a “one size fits all” approach to supply chain traceability. As such, this use case serves to generate new thoughts and provide direction by which one can derive great value specific to their individual organizational requirements for supply chain traceability within the Hyperledger universe.

For purposes of this specific use case, traceability will incorporate three “dimensions”, noted below. The three dimensions intersect to varying degrees and are required for robust supply chain traceability.

1. **End to end traceability** - gathering of all items required to develop the product to final delivery of said product to return of product.
2. **Product characteristics** - how is the product defined by industry, organizations, consumers, govt. etc.
3. **Regulatory concerns** - ensuring the traceable item meets compliance requirements.

Identifying the path by which the product makes its way from creation to end delivery is the basic construct required when fleshing out the details for supply chain traceability. An additional component of this dimension can be the need to follow a product back to its origin depending on the type of product. The complexity of following the end – end loop is increased exponentially in relation to the product’s characteristics. Finally, the laws and regulations affecting the product on its journey need to be identified and considered in regards to traceability.

Given the wide variety of possibilities for an organization’s product set, characteristics of a product vary widely. The spectrum of products is truly enormous. “Earth based products” such as diamonds, rare earth minerals or minerals from conflict zones are on one end of the spectrum, at other ends of the spectrum, there are sensitive electronics to tractors and jet aircraft.

An example of the complexity in regards to product characteristics follows. One organization produces individual electronic parts such as capacitors and resistors which are their products. Another organization uses those parts in a circuit board for their products. A third company builds a digital display, that incorporates the circuit board, for its product line. Finally, a tractor manufacturer incorporates the digital display into a series of trucks for consumer and corporate purchase.

Supply chain traceability challenges continue to increase when upgrades and repairs are performed. In many instances, a product may require an upgrade to its software or require upgraded parts and assemblies and new parts to repair failures. Issues stemming from improper software upgrades or malicious code are an increasing threat as technology advances in sophistication and automation. Counterfeit parts impugn the reputation of companies due to their inherent nature of being unreliable. In this vein, the counterfeits cause economic damage to the real producer.

Counterfeit parts are very real threat to the supply chain. “Sometime in the not-to-distant future, a submarine will sink. An air defense missile will detonate far from its intended target. [sic] directly result from a \$2 counterfeit electronic tucked deep within a billion-dollar military technology.”⁽¹⁾

Traceability and its relation to the law (e.g., regulatory law, international law etc.) has a profound effect upon many products. In the case of diamonds, conflict minerals or rare earth derived material several international agreements and global law governing these items. Ensuing traceability of these products can literally mean the difference between supporting terrorist groups or supporting those who need good jobs to provide for their family.

Environmental sustainability and the desire to ensure products are meet or exceed environmentally sound practices have a need for verifiable traceability. Traceability strategies or schemes related to sustainability are intertwined with industry consortium. Examples of these include the Forest Stewardship Council (FSC), the Marine Stewardship Council (MSC) or UTZ Certification. These consortiums provide “robust chain of custody standards and certification for products from the raw material to the final use phase.”⁽²⁾

Current Solution

While there are a variety of supply chain solutions and technology, the capability for ensuring traceability is commonly focused, to a varying degree, on specific links in the chain rather than across the full end – end supply chain (product creation to customer delivery to product return). In fact, during an MIT Center for Transportation and Logistics round table, a shipper noted, “... there are “many fragmented players, different technologies, lots of choices, and no single standard.”⁽³⁾

This situation is further exasperated by the inability to communicate product lifecycle traceability across the partner trading networks. The complexity found across the partner network, in the context of traceability, is extended in part through the varying needs of each participant in the network. The depth and proper definitions of governance is a major component required for a comprehensive functioning network. The technology interoperability and integration needs of each partner required to support individual traceability requirements leads to a variety of information silos unable to support the broader ecosystem.

Why Distributed Ledger Technology?

DLT provides a means by which every step in the supply chain can be readily tracked. Information dissemination of agreed upon parameters of a product or set of products provides the ability for multiple constituents (suppliers, producers, regulatory agencies, consumers etc.) to have verifiable provenance of the product. For instance, an abundant target opportunities for criminals exists costing "... U.S.-based semiconductor companies more than \$7.5 billion each year." ⁽⁴⁾

Using a consortium based model, DLT provides the ability to follow a product from inception to end point delivery while maintaining an appropriate degree of control and information availability to the consortium members. The three main components (end-end traceability, physical characteristics and regulatory concerns) can be properly accounted for through ensuring the permissions and access required of each entity (e.g., regulator, customer, partner, producer etc.)

Consider microchips. As noted above, counterfeit microchips cost multiple billions and a countless number of excellent paying jobs in the U.S. alone. The counterfeit process itself results in massive amount of environmental damage. One example of "reprocessing" is that the "reprocessors" often uses acid is used to strip microchips from a circuit board. The boards are slammed against a hard surface to quickly remove the part. Finally, a fake coating with fake laser etching is used to re-purpose the microchip.

The chips have now sustained damage invisible to the eye, there is simply no way to identify the extent of damage. The best-case scenario with a worst-case scenario leading to minor repairs with worst case scenario leading to catastrophic failure of an aircraft.

One method of eliminating the stopping chip counterfeits is to capture the location where the microchips were created and process the specific port of entry. If it is recognized the port of entry is a mismatch, the microchips would be held by customs and a notification sent to the appropriate parties detailing the counterfeit status. All these actions and processing are carried out via the Blockchain.

Opportunity/Justification

The current trace request process is started by a traceability partner, an end user inquiry or adverse event. The trace request initiator then follows the same path as the information flow and in some instances, may jump a step to contact Traceability Partners further up or down the chain to obtain the information. The traceability data source must also reply as quickly as possible to the enquiry and within the time frame governed by regulations and commercial agreements.

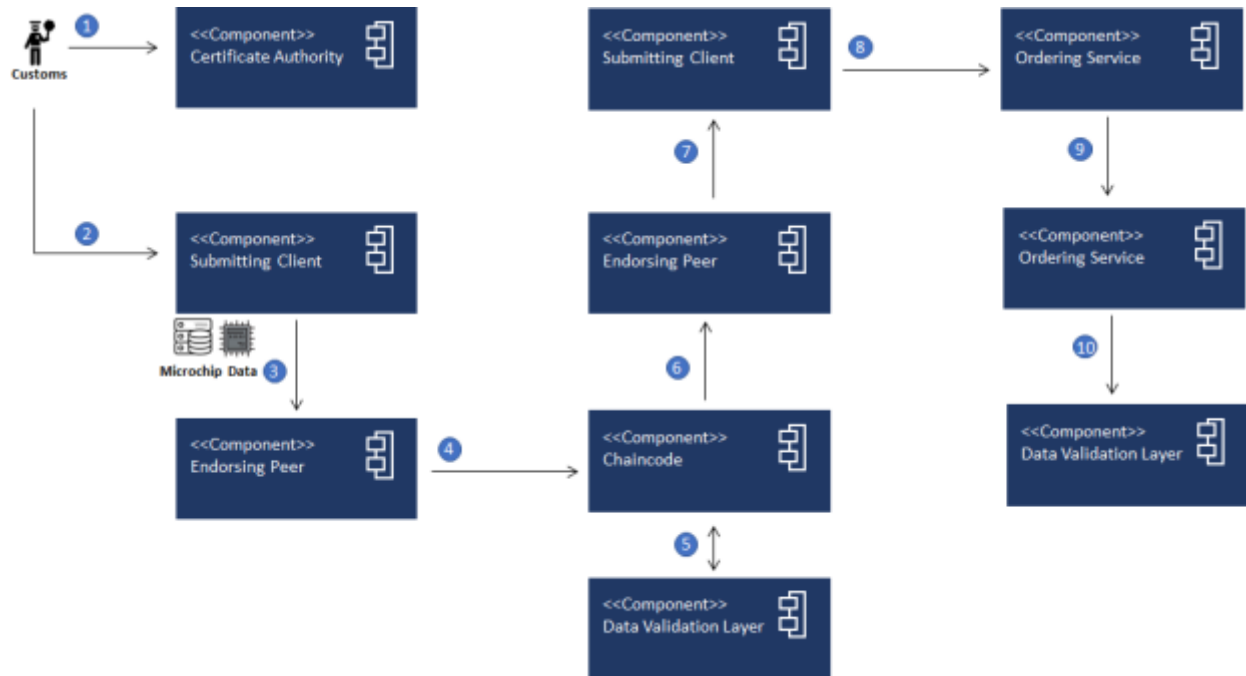
In one value add scenario, Blockchain provides almost instantaneous access for the request by allowing the requestor to access the trace data. From the blockchain, provided the permissions are in place, the requestor can navigate or view the required data to fulfill the request. In Hyperledger, the usage of chain code along with enacting controls for role based access and permissions enables the data to be segregated by the specific business need or designed for providing the data per its expected usage by the requestor.

In another value add scenario, Blockchain is used to thwart the damages caused by interjecting counterfeit items. The user story in section two illustrates this with a focus on counterfeit microchips but other areas of counterfeit fraud link back to the issue of improper software upgrades note earlier. “How can the maintenance crew on a U.S. aircraft carrier have absolute confidence that the software file they downloaded to 3D print a new part for a fighter jet hasn’t been hacked by a foreign adversary?”⁽⁵⁾

Other areas in which Blockchain can add real value include: provenance verification, incorporation of regulatory mechanisms that improve efficiencies across the supply chain. There are other opportunities by which Blockchain can be incorporate into a larger end-end architecture to derive additional benefits for the supply chain including: financial optimization optimized shipping costs, optimized taxes etc.

Section 2 - User Stories and Requirements

In this example, we demonstrate a user story based on shipping microchips from a company based in the Asia-Pac region to an end a set of microchips to the United States (US). The initial entry point for the microchips is a port of entry in San Diego. The chips are first inspected by customs prior to being sent on their way to the destination. All users in this story have a traceability role while some may assume a trading partner role. The chips themselves have unique markings that provide a tracking mechanism indicating the chips should have arrived from Europe and therefore causes US customs to become suspicious and flag the chips for further inspection. The following diagram is designed to elucidate an event flow of the use case.



Sample Hyperledger “Counterfeit Detection” Architecture

1. Customs entity is validated and enabled to perform a “counterfeit check”
2. Customs submits a “counterfeit check” request
3. Submitting client starts the “counterfeit check” via counterfeit recognition processing based on the received microchips and associated data
4. Endorsing peer enacts a ”counterfeit check” via Chain Code to validate product provenance and authenticity status
5. Chain code interacts with the Data Validation Layer to validate the microchip’s status
6. A possible counterfeit product is identified as the item has arrived in a San Diego, California Port from the APAC region, expected arrival Port was Miami, Florida from the EMEA region
7. Read/write set (possible counterfeit product) is delivered to the submitting client
8. A “counterfeit notification” transaction is endorsed and delivered
9. “Counterfeit notification” transaction delivered
10. “Counterfeit notification” data is stored on the ledger.

A data validation layer is shown which incorporates Fabric’s LevelDB, CouchDB along with other databases integrated into the architecture. As the product, has been identified as a possible counterfeit, additional flags can be passed to the data validation layer that would provide an automated means for Blockchain participants (e.g., buyers and OEM’s) to be alerted to predefined conditions as in the case of counterfeiting. Proven cases of counterfeiting will be efficiently processed enabling Blockchain participant’s full transparency of traceability partners.

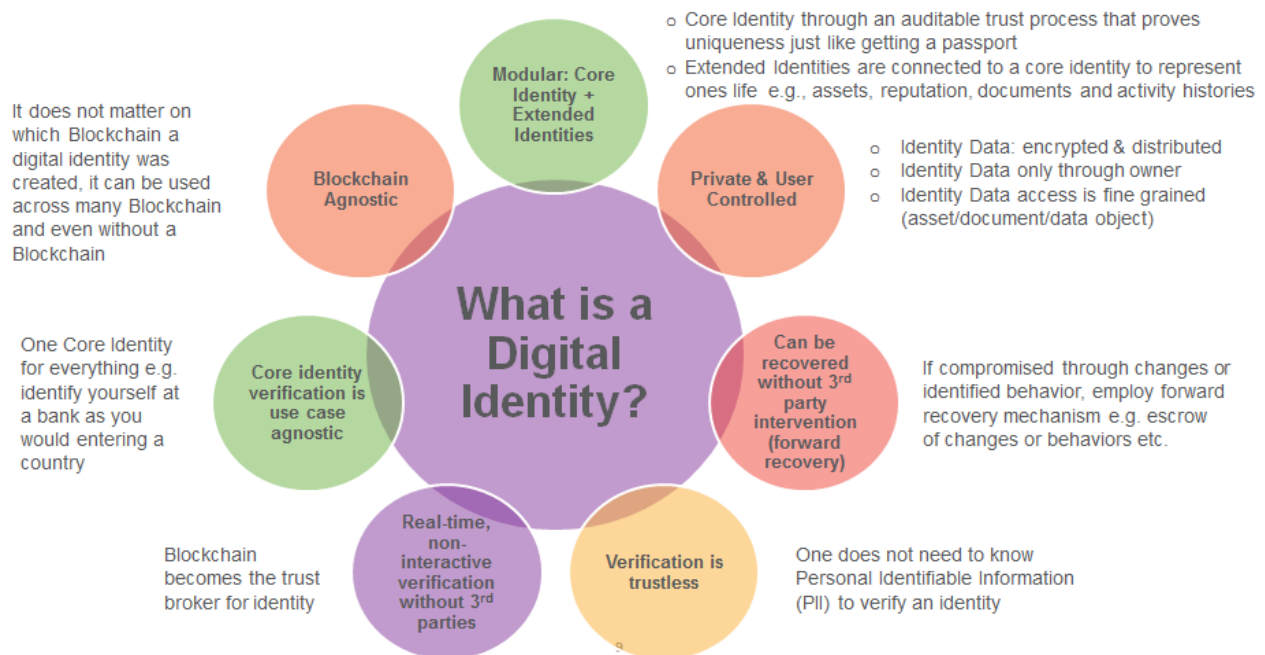
Key Concepts:

Seven key concepts: (1) core identity, (2) external data handling; (3) configuring permissions; (4) regulatory concerns; (5) hard asset linkage within DLT; (6) insurance; and (7) SLAs need to be accounted for within the scenario noted above. The concepts will be applicable across a variety of Supply Chain traceability uses and are therefore identified specifically within the next few paragraphs but are not detailed in this use case due to the various possibilities and incarnations that can come into play.

The first concept incorporates the idea of developing a core identity (i.e., unique identity) of an item. This identity defines what the asset, product or item is. For instance, in our scenario the core identity would be developed every lot of microchips with every new lot created with a new persona. Identities would be extended by capturing additional event information appropriate to the product (e.g., date/times of arrival, regulatory compliance information collection etc.) using a Digital Identity Protocol. Another means of developing a core identity is through the product owning every single lot (core identity) providing for unique products per lot. In this case data will be collected against each individual lot.

In practice, a chipset will have its own private/public key. A program is executed and then used to “sign” the chipset’s ID. As the chipset is processed through the supply chain, there will be a signing algorithm in place used to verify the chipset which is promulgated through the Digital Identity structure and is designed as platform agnostic.

Using either method for development of the core identity enables process data to be attached to the core identity which then provides the provenance traceability. As an example, an assembly may have the need for a software update maintenance event. The update is applied with the resultant updated recorded on the DLT, ensuring the traceability provenance. This individual actions (e.g., software update) are all recorded providing a clear picture throughout the asset’s lifecycle. The following *diagram provides a graphical depiction of a Digital Identity.



***TCS Patent Pending Digital Identity Component**

The second key concept involves data following the asset that has been defined, stored, altered etc. outside the Supply Chain Blockchain used for performing traceability. A multitude of trust issues could stem from external data when the Blockchain is functioning as expected. Even simple provenance issues such as inaccurate time stamps or improperly geotagging of products have the possibility of causing a catastrophic event (e.g., customers dying or taking ill from listeria that has found its way to your company's' spinach or an F-35 crashing due to counterfeit microchips).

In this concept, the Digital Identity of the data provider outside the Blockchain environment can be made known which can be trusted to ensure the data provider has been identified in the event issues arise with the data. Again, there is no provenance, accuracy or other DLT mechanism to ensure valid data has been introduced to the system from an external source. A Data Oracle can be one example of an invalid external source where this risk would need to be identified and mitigated.

The third key concept involves determining how permissions can be configured so that the right separation between public and private data is designed into the environment. While permissions scenario used in this document reflects the operations of a DLT between five entities (customs, buyer, seller, broker and OEM) there are multitudes of situations wherein architecting and building permissions suitable to a complex supply chain encompassing thousands of entities needs to be accounted for.

Suppliers would share information with the “parent” trading partner but have their information siloed via a channel (i.e., sub-ledger) enabling the data to be hidden from other competitors. If additional entities needed access for any reason, third party commercial lender, they could be added to the channel to access the information.

The fourth key concept concerns regulatory requirements that may or may not apply given to any traceability scenario. As the supply chain complexity increases around products, the likelihood of an increasing web of intersecting regulations becomes apparent. There are even instances where compliance with some regulatory requirements clashes with other regulatory requirements. Some industries such as food manufacturing or rare earth production have dedicated traceability schemes specialize by sub-industry. For instance, coffee producers have three Global Collaborative Traceability Schemes involved with coffee production.

Linking hard assets to DLT provides a real challenge and unique opportunities. Electronic and digital asset tracking within Blockchain can help with the design for hard asset tracking but counterfeiting or mislabeling hard assets presents a grand target for unethical companies and miscreants. One example of counterfeiting could be a company that completes an authentic production run of a given product, shutting the authentic run down and then performing a counterfeit production with details mimicking the authentic product. Another scenario involving mislabeling (much simpler to execute) involves swapping labels between parts to gain full monetary credit for returns. A factor driving these illicit activities is the greater the monetary opportunity, the greater the efforts and sophistication to counterfeit or mislabeling will be.

One mechanism that may provide an answer to the problem of counterfeiting in microchips involves a two-prong strategy. One prong would be developing pre-generated keys or software that can be embedded in the microchip. The other prong would involve incorporating Nano particles or other markers into the chips manufacturing process. Once the software and markers are integrated in the chip, corresponding “packages” reflecting the unique signatures of the markers and software can be loaded onto the Blockchain. When needed, a security check or interrogation of the package could be processed (e.g., running a hash to validate the chip’s code) to determine the chip’s authenticity.

Everledger is one company putting Blockchain (specifically Hyperledger) in use to provide traceability for diamonds. Everledger creates a 3D digital map and embeds these images on the chain. Later as needed, the images can be interrogated and used in proving the diamonds authenticity. Additionally, certificates of authenticity proving the origination details for the diamond are stored in the Blockchain which makes their ability to verify the source transparent and unalterable.

The sixth concept noted in this paper, SLAs, provides a good way to incorporate Blockchain functionality within the organization. This is a low risk area to perform POCs and gather the knowledge of capabilities offered through Blockchain for developing a grand strategy for DLT.

Benefits provided by SLAs integration with DLT include automated tracking mechanisms that prove the consistency of service. Companies can use this information as a bragging point for the provider or a clear value add proving (transparently thanks to Blockchain) the provider has high SLA compliance. This compliance can be a crucial factor to winning new business in industries where high SLA compliance is a must have. Contract negotiation could well benefit by the creativity of the negotiators using the transparency of Blockchain to trigger bonus payments, extensions or level fines based on the ability of the provider to maintain SLAs.

Just as Blockchain is eliminating friction in Fintech, Blockchain can build in efficiencies that eliminate the drag on ensuring compliance with the SLAs through automation. Payments integrated with proven SLA compliance through Smart Contracts have the possibility of eliminating human based decisions in determining if the SLAs were met. In fact, any area where humans are involved in the SLA structure should be investigated for improvement with DLT.

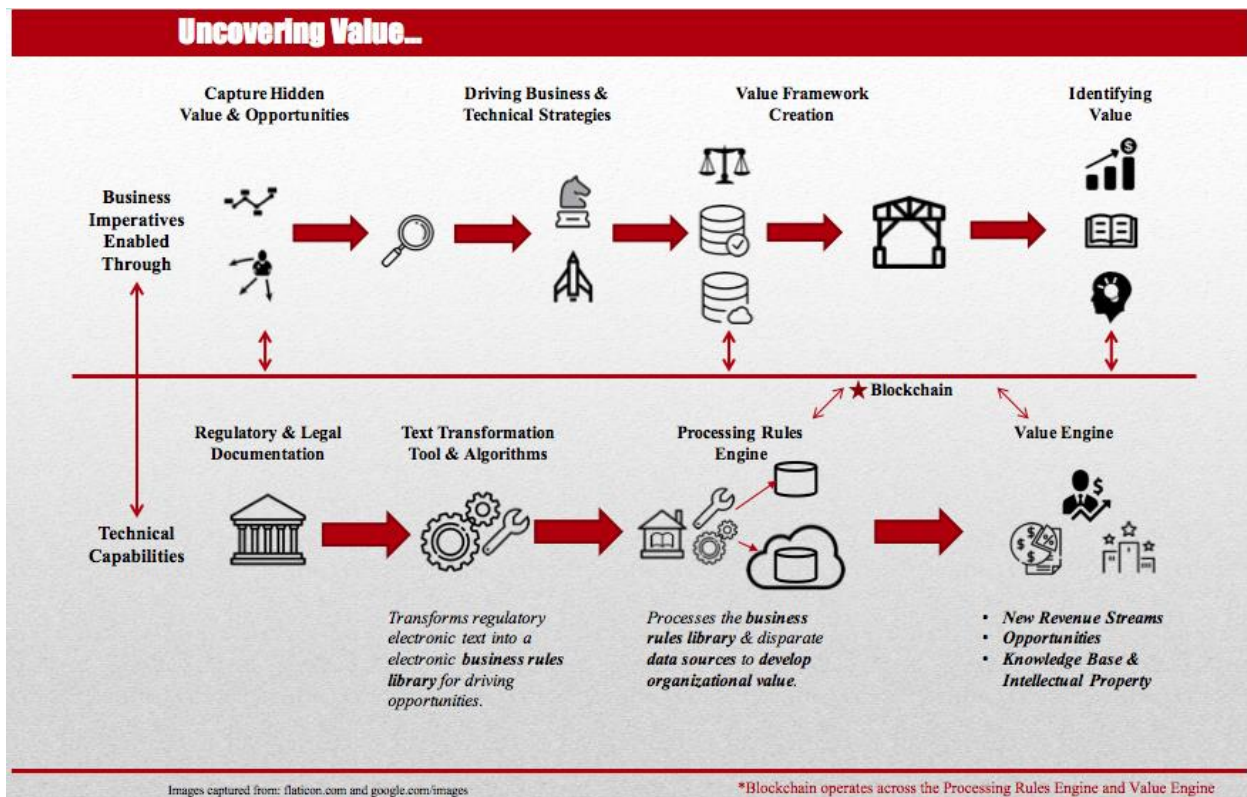
The insurance industry, the seventh key concept, has recognized the need for DLT to evolve with the new business environment and changing regulatory conditions. In fact, an insurance industry consortium has been launched by the two largest reinsurers (Munich Re and Swiss Re) to identify the value of DLT and plan.

Claim processing times will dramatically increase as Smart Contracts will be engaged to eliminate the “friction” inherent in working through the negotiations of determining what company is responsible for the various clauses in contracts and thereby provide a more equitable and transparent system for determining a company’s financial and contractual obligations. Transparent and consistency in contract language and structure will be provided by DLT and stored on it which will eliminate questions caused by the existence of multiple contract versions.

Providing customer flexibility through creativity in designing insurance to meet unique customer needs is another mechanism by which Block Chain can dynamically evolve the industry. Currently many companies pay a blanket amount of insurance for storage regardless of what is being stored, how much is being stored etc. By using IoT with Blockchain, insurers could provide a smart monitoring option to dynamically adjust coverage levels, costs and eventually offer better pricing to their clients. Parameters used in this scenario could include: (1) RFID identification of assets or products stored at the location; (2) incorporation of current security RFID schemes and structures; (3) personnel security identification (exit and entering building); (4) environmental variables such as humidity and temperature; and (5) asset transfer scheduling (in or out of the building).

As noted in the SLA section above, any area where humans are involved in the process should be investigated for improvement with DLT. Using code (which is transparent to all organizations involved) making can drive efficiencies and ensure better decision making through a Blockchain Business Rules Engine.

Blockchain capabilities can be expanded with additional technical components to provide a complete end - end architecture that layers in the Hyperledger Fabric as a Processing Rules Engine. The engine would enact various transactions based on chain code algorithms that were driven from the regulatory rules loaded in the engine. In this manner, the Blockchain participants would can ensure regulatory compliance. An additional value add will be through providing the ability to extrapolate benefits through identifying revenue sources, tax optimization and more using the Hyperledger Fabric as a Value Engine where multiple data science techniques can be applied against the Value Engine. The following diagrams illustrates this scenario.



High Level Block Chain Value Engine Architecture

Some additional context to the scenario described below is that external traceability exists when an item is transferred from on traceability partner to another. In this example the shipper acts as a traceable item source and the customer is supposed to be the traceable item recipient.

User Rubric:

User	As a...	Wants to....	Because....
Customs	Government entity	Identify counterfeits parts	They are tasked with identifying counterfeit items and stopping them from entering the US.
*Traceable Item Source	The microchip sourcing entity	Sell and ship counterfeit microchips	Are a criminal element.
Traceable Item Recipient	The purchasing entity	Purchase supposedly good microchips	They have identified a lot of microchips that have come up in the grey market making it worth the customer's while to purchase the chips.
OEM	Original manufacturer	Identify and track large lot purchases	Ensure they can enforce contractual obligations of their partners in addition to understanding developing data for understanding the efficacy of their counterfeiting countermeasures.
**Broker	Intermediary between the shipper and customer	Entity whereby a previously unknown	They receive a commission based on the purchase of the microchips for finding a buyer.

*The shipper is a criminal actor but is a definite user within this scenario.

**Broker may not be a criminal actor but at a minimum should be held some share of responsibility as they should have known the shipper was providing counterfeit parts.

Section 3 - Requirements Not Related to User Stories

The following requirements used the GS1 Global_Traceability_Standard ⁽⁶⁾ as a foundation.

General traceability requirements include:

- The traceability partners can (one step up, on step down):
 - Track the item back to the partner that sent the part
 - Follow the path of the item to the next direct traceability partner receiving the part

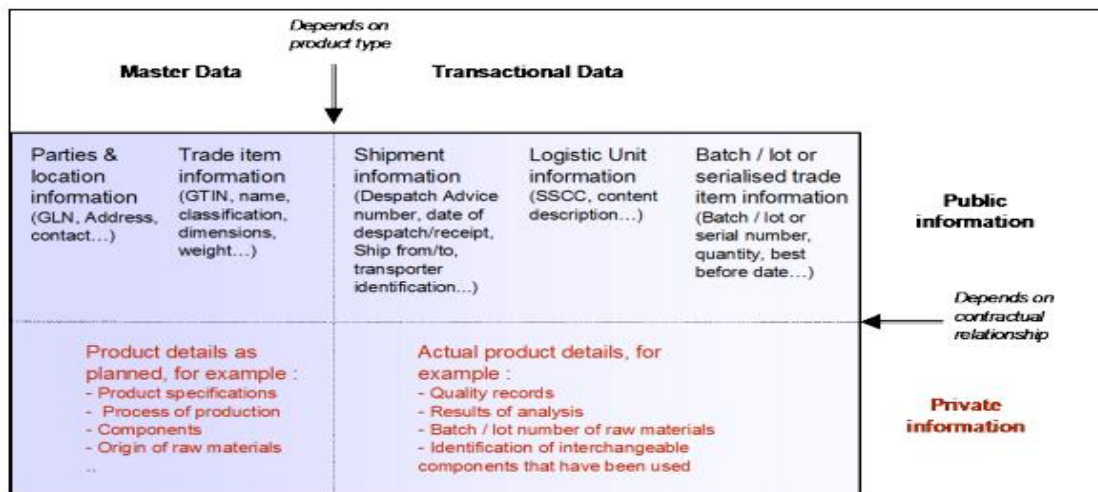
Information flows:

- Provide a separate track for information flows (one up, one down principle)
 - Minimum amount of data that is recorded across Traceability Partners
 - Ensure visibility and linkage across all appropriate levels
 - Additional information defined by the network is recorded and shared

Assumptions for the traceable item matrix/hierarchy include:

- Traceable items may need batch/lot physical number based on certain regulations
- Where needed, a best before date should be added, e.g., fresh food
- As the traceable precision level increases a serial number may need to be incorporated
- A serial number may be appropriate for items not crossing the point of sale that need to be traced at this level.

Data Requirements:



General Traceability Data Requirements:

Logical Grouping:	Data Type:
Who: Traceability Partners (ID and data elements)	Master Data
What: item (ID and data elements)	Master Data
Where: location (ID and data elements)	Master Data

*What occurred: process of events	Event or Operational Data
When: dates and times	Event or Operational Data

*At this time, remains undefined due to the variety of possible events.

Master Data:

Logical Grouping:	Data Field:
Who (Traceability Partner)	Global Location Number (see glossary)
	Entity Name
	Entity Point of Contact
	Entity Street
	Entity State/Province
	Entity Zip Code/Postal Code
	Entity Country
What (Trade Item)	GTIN
	Batch/Lot
	Shipping Container Height
	Shipping Container Weight
	Shipping Container Length
	Weight
	Name
	Product Description
Where (Location)	Location Gestapo

Event Transactional Data:

Logical Grouping:	Data Type:
When (Timing)	Planned time

	Expected time
	Actual time
	Planned Date
	Expected Date
	Actual Date

General Data Characteristics:

1.	Master data is relatively consistent.
2.	Transactional data is independent from day to day according to the physical events.
3.	Location identification precision level defined by the traceability partner (e.g., warehouse location down to a precise bin location in the warehouse).
4.	Must be defined with appropriate governance rules prior to physical flow of items.
5.	Private details (which are defined in the contract) can include: <ul style="list-style-type: none"> - product specifications - process of production - components - raw material origin.
6.	Event or transactional data: <ul style="list-style-type: none"> - created during physical flow of goods - collected when events occur.

Characteristics of Locations Identification:

1.	Must be uniquely identifiable.
2.	Location identification precision level defined by the traceability partner (e.g., warehouse location down to a precise bin location in the warehouse).
3.	Must be globally identifiable.

Characteristics of Trading Partners Identification:

1.	Have globally recognized identification.
2.	Be uniquely identified.

3.	Have identification precision level defined by the traceability partner (e.g., Legal Entity).
----	---

Characteristics of Product/Item Traceable Identification:

1.	Must be globally identifiable.
2.	Must be uniquely identifiable.
3.	Must have items identification applicable to all product hierarchy levels as appropriate.
4.	Must be assigned at the latest when physically created.
5.	Must at a minimum have GTIN identification for trade items.
6.	Varying precision level required depending on the item (e.g., more precision spreading from batch/lot number to serial number/SGTIN).
7.	Identification precision level defined by the traceability partner.
8.	Logistics units must be uniquely identified (e.g., serial shipping container code specifications).
9.	All traceable items must carry identifiers on the asset containing it or accompanying documents.
10.	Best practices dictate using a human readable form in the most appropriate location (e.g. on the product or with the product documentation etc.).
11.	Identification carrier must remain on or attached to the traceable item when packed in an upper level of packaging.

Section 4 - External References and Glossary

Cited Quotes:

1. <http://www.businessinsider.com/technology-is-a-huge-national-security-threat-2013-8>
2. https://www.unglobalcompact.org/docs/issues_doc/supply_chain/Traceability/Guide_to_Traceability.pdf
3. <https://knowthechain.org/the-logistics-of-tracking-traceability/>
4. https://www.semiconductors.org/clientuploads/directory/DocumentSIA/Anti_Counterfeiting_Task_Force/ACTF_Whitepaper_Counterfeit_One_Pager_Final.pdf

5. <https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain>
6. http://www.gs1.org/sites/default/files/docs/traceability/Global_Traceability_Standard.pdf

Another Researched Works:

<http://searchmanufacturingerp.techtarget.com/feature/Blockchain-not-a-panacea-for-supply-chain-traceability-transparency>

<https://www.provenance.org/whitepaper>

[Handbook of Research on Global Supply Chain Management](#)

https://www.unglobalcompact.org/docs/issues_doc/supply_chain/Traceability/Guide_to_Traceability.pdf

<http://www.defenseone.com/technology/2013/08/counterfeits-can-kill-us-troops-so-why-isnt-congress-and-dod-doing-more-stop-it/68381/>

<https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain>

<https://blog.michaeldowling.me/the-upcoming-fabric-1-0-release-6271809d023>

<http://www.thingmagic.com/index.php/rfid-security-issues>

Glossary:

Logical Grouping:	Data Type:
Global Location Number (GLN)	The GS1 Identification Key used to identify physical locations or legal entities. The key is comprised of a GS1 Company Prefix, Location Reference, and Check Digit.
(GTIN) The GS1 Identification Key used to identify trade items.	The GS1 Identification Key used to identify trade items. The key is comprised of a GS1 or U.P.C. Company Prefix followed by an Item Reference Number and a Check Digit.